

Durante los últimos años, la aparición de noticias sobre amenazas a la privacidad en Internet, que afectan tanto a empresas como a personas, ha despertado la conciencia en una parte muy significativa de la sociedad respecto a la importancia que tiene proteger la información en un mundo digital.


Se trata además de una situación compleja, en la que el número y la variedad de ciberamenazas es cada vez más elevado dado el proceso de digitalización de toda la economía y el avance de nuevas tendencias tecnológicas, como la computación en la nube o el Internet de las cosas. Este monográfico, editado por Fundación Telefónica, ofrece una visión global de estos y otros temas, y de cómo se puede abordar la seguridad en el mundo digital, área que denominamos "ciberseguridad".

Se aborda este fenómeno de una forma global tratando de incorporar diferentes perspectivas, teniendo en cuenta el punto de vista de los usuarios tradicionales de Internet, el de las empresas, tanto las que utilizan como las que crean las tecnologías, y también el de las Administraciones. En el informe se destaca la forma en que las nuevas tendencias tecnológicas, como la computación en la nube, el Internet Industrial o la difusión masiva de *apps*, suponen un desafío importante que obliga a replantear los modelos tradicionales de seguridad e incluso repensar el propio concepto.

Al igual que sucede con otros informes de esta colección, el trabajo inicial se complementa con la realización de un *think tank* en el que numerosas personalidades de referencia en diferentes campos del conocimiento ofrecen su visión del tema. Estas conversaciones han sido transcritas de forma literal e incluidas en el estudio, lo que enriquece el informe y le confiere un mayor valor añadido.

Ciberseguridad, la protección de la información en un mundo digital



A dark blue circle is centered on the page. Inside the circle, the text "Comparte esta publicación en redes sociales:" is written in white, sans-serif font.

Comparte esta publicación
en redes sociales:

CIBERSEGURIDAD, LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL

CIBERSEGURIDAD, LA PROTECCIÓN DE LA INFORMACIÓN EN UN MUNDO DIGITAL

Esta obra ha sido editada por Ariel y Fundación Telefónica en colaboración con Editorial Planeta, que no comparten necesariamente los contenidos expresados en ella. Dichos contenidos son responsabilidad exclusiva de su autor.

© **Fundación Telefónica, 2016**

Gran Vía, 28
28013 Madrid (España)

© **Editorial Ariel, S.A., 2016**

Avda. Diagonal, 662-664
08034 Barcelona (España)

© de los textos: Fundación Telefónica.

© de las ilustraciones de cubierta: © Hywards-Shutterstock

© MaximP- Shutterstock © Maksim Kabakou-Shutterstock

Coordinación editorial de Fundación Telefónica: Rosa María Sáinz Peña

Primera edición: Septiembre de 2016

El presente monográfico se publica bajo una licencia Creative Commons del tipo: Reconocimiento - Compartirlgual



Esta obra se puede descargar de forma libre y gratuita en:
<http://www.fundaciontelefonica.com/publicaciones>

ISBN: 978-84-08-16304-6

Depósito legal: B.16.537-2016

Impresión y encuadernación: UNIGRAF, S.L.

Impreso en España – Printed in Spain

El papel utilizado para la impresión de este libro es cien por cien libre de cloro y está calificado como **papel ecológico**.

Índice

Introducción	XI
1. Identidad, privacidad y seguridad en el nuevo entorno digital	1
1.1 Mundo digital: un mundo basado en la información	3
1.2 Identidades digitales frente a identidades físicas	6
2. Los ciudadanos y empresas, ante la seguridad y privacidad	9
2.1 El internauta, ante la privacidad y la seguridad	10
2.1.1 Actitudes ante la privacidad	10
2.1.2 Actitudes ante la cesión de datos personales para obtener beneficios	12
2.1.3 Ciberamenazas a la privacidad de los usuarios	13
2.1.4 Medidas relacionadas con privacidad y seguridad tomadas por los usuarios	14
2.2 La empresa, ante la privacidad y la seguridad	15
2.2.1 Ciberamenazas a la privacidad y seguridad de las empresas	15
2.2.2 Medidas relacionadas con privacidad y seguridad tomadas por los usuarios	16
3. El ciclo de vida de la ciberseguridad	19
3.1 Prevención	21
3.1.1 Control de accesos y gestión de identidades	21
3.1.2 Prevención de fugas de datos	25
3.1.3 Seguridad de red	27
3.2 Detección	28
3.3 Respuesta	30
3.3.1 Sistemas de recuperación	32
3.3.2 Evidencias digitales / cumplimiento con la regulación	34
3.4 La inteligencia para dotar de eficiencia a las medidas de ciberseguridad	35
3.4.1 Análisis de información proveniente de fuentes diversas y búsqueda de correlación	35
3.4.2 Fuentes de datos abiertas (OSINT–Open Source Intelligence)	36

3.4.3	<i>Profiling</i> de usuarios–Atribución	37
3.4.4	Compartición de datos de incidentes entre corporaciones	38
3.4.5	Diversidad de estándares	40
4.	Nuevos escenarios y desafíos de la ciberseguridad	43
4.1	BYOD (<i>Bring Your Own Device</i>)	44
4.1.1	Necesidades de seguridad	45
4.1.2	Soluciones de seguridad	46
4.2	Cloud computing y big data	47
4.2.1	Necesidades de seguridad	47
4.2.2	Soluciones de seguridad	50
4.3	Internet de las cosas (<i>Internet of Things</i>)	51
4.3.1	Necesidades de seguridad	52
4.3.2	Soluciones de seguridad	53
4.4	Internet industrial	54
4.4.1	Necesidades de seguridad	56
4.4.2	Soluciones de seguridad	57
4.5	Apps móviles	58
4.5.1	Necesidades de seguridad	59
4.5.2	Soluciones de seguridad	60
4.6	Múltiples identidades digitales: el reto para protegerlas e identificarlas con la identidad física	61
4.6.1	Necesidades de seguridad	62
4.6.2	Soluciones de seguridad	63
4.7	Desafíos legales de la ciberseguridad	65
5.	Transcripción del encuentro de expertos en ciberseguridad	71
	Reunión de expertos en ciberseguridad	72
	Introducción	73
	Miguel Pérez Subías	77
	Paloma Llana	81
	Elena García Díez	87
	Manuel Escalante García	95
	Carlos Abad Aramburu	103
	José Valiente	111
	Antonio Guzmán	117
	Ángel León Alcalde	123

Introducción

Internet es una realidad que nos envuelve completamente, cada vez hay menos espacio que quede a su margen, y menos quedará en los próximos años. El ocio, el trabajo, las comunicaciones... absolutamente todas las actividades que realizamos están en cierto modo impregnadas de un carácter digital que hace que la información sea fácilmente grabable, reproducible, y cómo no, también puede escapar de nuestro control, caer en las manos de quien no debe y en última instancia ser utilizada en nuestra contra.

Nos encontramos por tanto en una situación en la que las tecnologías hacen mucho por nosotros, eso nadie lo duda, pero también en la que pueden suponer un problema, al menos para algunos de nuestros valores fundamentales. Y es que durante los últimos años ha sido más habitual de lo que debiera el que información sensible haya escapado del ámbito de los usuarios y de las empresas, lo que ha generado una alarma muy importante. De hecho, según muestran estudios internos cuyos resultados mostramos en el presente monográfico, el 82,8 % de los internautas considera que este tema tiene una gran importancia, entendiendo privacidad en un sentido amplio que incluye la información personal como fotografías y vídeo y los datos personales, y también otra información como el historial de páginas web o el historial de búsquedas realizadas.

Es más, el 85,2 % de los internautas afirma que debería ser posible identificar y borrar los datos personales de Internet si así lo desea y el 62 % que debería ser posible mover los datos a otra plataforma o red social. Nos encontramos, por consiguiente ante una demanda de los usuarios con respecto a la seguridad y privacidad que en muchos casos no es ofrecida por las empresas y organizaciones que operan en el mundo digital.

Se trata de un momento importante, en el que el mundo tecnológico está cambiando profundamente, lo que tiene implicaciones en el entorno, las relaciones entre las personas, en los trabajos, el ocio... En esta situación la información se convierte en la principal materia prima de los servicios digitales y también se convierte en un recurso que hay que controlar. Llama la atención cómo ante este nuevo escenario, completamente diferente al de hace unos años, la mayoría de los usuarios siguen recurriendo al antivirus como herramienta principal y a veces única para confiar su seguridad, lo que es ahora completamente insuficiente. Destaca cómo la mayoría de los usuarios, por tanto, siguen recurriendo a modelos pasivos para controlar su seguridad a excepción de algunos comportamientos activos como desconectar o tapar la webcam, hábito que ya tienen el 43 % de los internautas, el 45,7 % en el caso de las mujeres y el 54,4 % en los jóvenes entre 20 y 24 años.

Existe, así, en la actualidad un déficit respecto a la realidad y las necesidades en cuanto a seguridad en el mundo digital se refiere. Lejos de ser una brecha que se esté cerrando, este

monográfico analiza con profundidad los nuevos desafíos que empiezan a aparecer en el horizonte y que crearán todavía más tensión en el mundo de la seguridad y de la privacidad.

Así, el Internet de las cosas y más en concreto el Internet Industrial, tendrán como consecuencia el que todo esté conectado a Internet, desde nuestra ropa hasta los electrodomésticos de nuestra casa, creando todo un torrente de información que debe ser controlado para evitar que nuestra sociedad se convierta en un Gran Hermano en el que la privacidad e intimidad queden reducidos y se conviertan en la excepción en vez de en la norma.

Otras tendencias como la computación en la nube, según la cual la computación y el almacenamiento de datos se producen de una forma desacoplada con el espacio físico en el que se entrega el servicio, supone un importante desafío al cruzar la información las barreras transnacionales y con ello estar sometida a diferentes legislaciones, algunas de ellas menos restrictivas. La movilidad y utilización masiva de apps también genera una corriente continua de datos entre los que se incluye la geolocalización, que, combinados, pueden suponer problemas importantes para la privacidad de los usuarios.

Nos encontramos ante una revolución, más que una evolución, una revolución que afectará a todo el ecosistema relacionado con la sociedad de la información y que requerirá la implicación de todos para encontrar las mejores alternativas. Queda claro que el enfoque actual y las medidas que se están llevando a cabo en materia de seguridad y privacidad son insuficientes en el nuevo entorno digital que empieza, por lo que tenemos ante nosotros el reto de concienciar e involucrar a actores de diferente naturaleza y con distintas metas como usuarios, empresas tecnológicas, empresas finales y Administraciones. No tenemos ninguna duda de que una apuesta por la seguridad, que la tenga en cuenta desde el diseño de los propios servicios, será fundamental para el desarrollo robusto de la Sociedad de la Información que permita ofrecer una cantidad ingente de beneficios sin restar derechos individuales a las personas.

Identidad, privacidad y seguridad en el nuevo entorno digital

- 1.1 Mundo digital: un mundo basado en la información 3
- 1.2 Identidades digitales frente a identidades físicas 6

Una de las condiciones fundamentales para que un sistema social funcione reside en el desarrollo de toda una estructura de garantías que permita que las personas y organizaciones que operen en dicha estructura puedan garantizar su identidad y, también, otra información relevante en su vida, como cuáles son sus pertenencias, ya sean físicas o simplemente derechos; sus titulaciones, el haber sido ellos los que han realizado ciertas actividades... En definitiva, toda sociedad lleva aparejado un sistema de gestión de información que permite identificar a los miembros que la componen y recoger muchas de las interacciones que se producen entre ellos. Así, si una persona va al banco a retirar dinero, el banco debe ser capaz de identificar a la persona, de comprobar que tiene dinero y de anotar la operación para que conste que ese dinero ha sido retirado. Lo mismo sucede a la hora de realizar cualquier gestión con la Administración u otras organizaciones.

Una parte muy importante en la gestión de esta información ha corrido tradicionalmente a cargo de las Administraciones, que de esta forma garantizaban la identidad y otras informaciones fundamentales de las personas y organizaciones. Conseguir que todo este sistema funcionara de forma fiable ha supuesto siempre una gran cantidad de procedimientos, generalmente bastante rígidos, que han dado una importancia fundamental a acreditar la identidad de las personas y para los que han utilizado diversos tipos de recursos: fotos, fotocopias compulsadas, certificados, rasgos biométricos..., que en muchas ocasiones requieren realizar las actividades presencialmente. La incorporación de sistemas informáticos en este proceso supuso nuevas posibilidades que en muchas ocasiones han tardado en aprovecharse, ya que ha sido necesario un proceso de adaptación de los procedimientos.

En la actualidad estamos viviendo un cambio todavía de mayor calado gracias a la generalización del uso de Internet, la digitalización de la economía a todos los niveles y la aparición de nuevas tecnologías, como la computación en la nube. Una revolución más que una evolución, una transformación global de la economía en la que los datos y la información son la nueva materia prima. Así, los usuarios, tanto personas como empresas, son capaces de darse de alta de forma inmediata, relacionarse con las Administraciones, interactuar entre ellos, muchas veces implicando transacciones económicas, sin salir de casa y utilizando en muchas ocasiones las contraseñas como única forma de garantizar la identidad.

Este nuevo entorno ha permitido el crecimiento exponencial de la economía digital, pero también ha supuesto problemas de seguridad, como la captura de contraseñas que ha llevado a que se hayan producido casos de robo de dinero o de usurpación de la identidad de usuarios. Las personas y organizaciones han ido adquiriendo mayor conciencia de esta situación a medida que el número de actividades que se realizan de forma digital ha ido aumentando y han ido adquiriendo una naturaleza más económica. Por ejemplo, un 43 % de los internautas hacen sus compras por Internet¹ o un 96 % de los trámites que las empresas

1. Datos de Telefónica.

realizan con la Administración se llevan a cabo utilizando para ello el formato electrónico². Los continuos escándalos que se han producido en los últimos meses y que afectan tanto a personas como a empresas han agudizado la preocupación por los temas relacionados con la seguridad.

Nos encontramos en un momento en el que la mayoría de la sociedad comienza a ser consciente de que la tradicional manera de abordar la seguridad en el mundo digital empieza a no ser suficiente, pues no ofrece soluciones ante las nuevas situaciones. Además, el proceso actual de digitalización de la economía, que incluye al sector industrial, y las nuevas tendencias tecnológicas provocan que sea una obligación el repensar desde el principio el concepto de ciberseguridad. Este estudio trata de ofrecer una visión global de la ciberseguridad, al mostrar las tendencias actuales y los desafíos que se deben afrontar en un futuro próximo para que el mundo digital sea un entorno seguro que inspire la confianza necesaria para impulsar nuevas inversiones por parte de las empresas y su adopción por parte de los usuarios.

1.1 Mundo digital: un mundo basado en la información

En la actualidad, casi todos los usuarios son conscientes de los beneficios que aporta Internet y la mayoría lo considera una puerta al mundo que proporciona a su vida un número interminable de posibilidades. Estos beneficios pueden ser prácticos, como el acceso a información, un ahorro de tiempo o una disminución de costes, y también emocionales, como mantener el contacto con los seres queridos, socializarse o tener un canal para expresar sus ideas. Se trata además de beneficios que no se reducen a un terreno concreto de su vida, sino que abarcan todos los campos. Así, en el ámbito del trabajo, parece impensable un entorno que no se beneficie de la inmediatez en las comunicaciones y el acceso al conocimiento y la información que brindan estas tecnologías; en el ámbito social, los diferentes modos de comunicación que han emergido en la web han conducido a un cambio radical en la esfera social y han marcado un antes y un después en cómo entendemos las relaciones interpersonales, la expresión personal y la privacidad; en el terreno del entretenimiento, el acceso al entorno global ha incrementado exponencialmente la oferta.

En todos estos entornos, los datos son la materia prima fundamental utilizada en la construcción de los servicios digitales. Así, en un mundo digital, las identidades, las transacciones, los contenidos..., son datos digitales que se pueden reproducir y transmitir fácilmente. En un ámbito que se concibe de forma abierta como Internet, esta situación ha sido aprovechada en muchas ocasiones por hackers y otros ciberdelincuentes. Ante esta situación, los usuarios empiezan a tomar ciertas precauciones a la hora de compar-

2. Boletín de indicadores de Administración Electrónica, mayo 2015 del OBSAE.

tir los datos; de esta manera, estudios realizados por Telefónica muestran que muchos usuarios están adaptando sus comportamientos, por ejemplo, no accediendo desde ordenadores públicos a sus cuentas bancarias o comprando online solamente en páginas web de empresas bien conocidas. En otros casos, algunos usuarios han llegado a suprimir ciertos comportamientos como el chequeo en servicios de localización o dejar comentarios en medios sociales. Estas actitudes muestran que los usuarios empiezan a tener una cierta conciencia respecto a los datos que comparten y que se generan en su actividad en Internet.

A este respecto, se debe tener en cuenta que no todo lo que se comparte en la utilización de los medios digitales se hace conscientemente, y que incluso en muchas ocasiones es imposible evitar el compartir gran cantidad de información cuando nos conectamos a Internet y utilizamos sus servicios. La figura 1.1 muestra los tres tipos de información que se producen por la actividad en la red. En todos ellos, los usuarios tienen importantes dudas respecto a cuál es su destino final y quién tiene acceso a ellos.

- *Información que se comparte por defecto.* Solamente los usuarios avanzados conocen que la mera interacción con diferentes dispositivos y plataformas y actividades sencillas como realizar búsquedas generan información que queda registrada. La mayoría de los usuarios piensan que dicha información se encuentra solo en el dispositivo o que desaparece al finalizar la sesión.
- *Información que se comparte de forma forzada.* Todos los usuarios son conscientes de que es necesario introducir cierta información con la intención de acceder a los beneficios que ofrece la web. Firmar en plataformas, compartir datos personales o proporcionar un número de cuenta bancaria son algunos de los pasos lógicos que es necesario abordar para acceder a los servicios o llevar a cabo transacciones. Los usuarios creen que esta información se queda en la plataforma o website que ofrece el servicio, que es responsable de su uso gracias a las leyes que aseguran la privacidad de los datos. La mayoría de los usuarios no son conscientes de los términos que la mayoría de los servicios y aplicaciones obligan a firmar respecto a la utilización de sus datos.
- *Información que se comparte de forma voluntaria.* Esta voluntariedad va asociada generalmente con el contenido generado por el usuario (redes sociales, comentarios en foros, emails...) como una muestra de expresión de sus opiniones. Los usuarios son conscientes de que es información que queda expuesta a los demás e información que tiene un gran contenido emocional, lo que en algunas ocasiones puede ser utilizado en su contra. En estos casos consideran que su privacidad está en peligro, pero tampoco conocen cuál es el ciclo de vida de dicha información ni las reglas que aplican para proteger su privacidad.

Figura 1.1 Formas de generar y compartir la información en Internet



Fuente: Elaboración propia.

Además del grado de voluntariedad, es necesario tener en cuenta que no toda la información posee el mismo nivel de sensibilidad. Hay información que en condiciones normales no debería suponer un problema para los usuarios, como la navegación en sitios web o de contenido neutro o bajar información de dichos sitios o, por ejemplo, las búsquedas relacionadas con productos, viajes o restaurantes. Sin embargo, otro tipo de información que se comparte en Internet tiene una sensibilidad que hace que sea peligroso que caiga en manos de personas y organizaciones que puedan hacer un uso ilícito de ella; en este grupo se encontrarían los datos personales, como la dirección o los detalles de las cuentas bancarias. Entre estos extremos se sitúa otra información que puede volverse «delicada» en ciertos contextos, como comentarios políticos, fotos privadas, visitas a sitios web sobre sexo, problemas de salud...

De esta forma, la combinación de estas dos variables, grado de voluntariedad y sensibilidad, es fundamental a la hora de definir la actitud ante la privacidad en los servicios digitales. La figura 1.2 muestra de una manera general, sin entrar en detalles ni casos particulares, cuál puede ser la actitud más interesante para cada una de las combinaciones.

Figura 1.2 Actitud ante la seguridad y privacidad dependiendo de la voluntariedad y sensibilidad de la información



Fuente: Elaboración propia.

1.2 Identidades digitales frente a identidades físicas

El concepto de identidad humana puede definirse como el conjunto de rasgos que hace a una persona ser quien es y la distingue de las otras al mismo tiempo que le permite interactuar en su entorno. La formación de la identidad es un proceso que comienza a configurarse a partir de ciertas condiciones propias de la persona, presentes desde el momento de su nacimiento y que, desde ahí, va evolucionando según los hechos y experiencias que le van aconteciendo a lo largo de su vida. La identidad se configura a partir de la interacción con el medio y el funcionamiento individual propio del sujeto, que forma entre ellos una tensión dinámica que guía la configuración de la identidad hacia una dirección determinada. La identidad se modifica a lo largo de la vida y su desarrollo se realiza en función de la interacción con el medio externo, ya que en una situación de aislamiento, las características individuales resultan irrelevantes. Así, es precisamente en relación con la interacción con los otros cuando las diferencias y características individuales adquieren valor e importancia. En la tabla adjunta se recoge un resumen de los elementos clave que ayudan a entender en qué consiste la identidad humana.

Tabla 1.1 Elementos clave de la identidad humana

<p>La identidad humana es lo que define a la persona y la distingue frente a los otros</p> <p>Se construye plenamente en función de las condiciones de la propia persona, pero también en función de hechos y experiencias vividas:</p> <ul style="list-style-type: none"> • Relaciones con otros (cruce individuo-grupo-sociedad) • Historia de la propia vida • Historia social <p>La identidad humana solo se realiza en función de la interacción con el medio externo</p> <p>Evoluciona a lo largo del tiempo</p> <p>La necesidad de un sentimiento de identidad es vital e imperativa para el hombre</p>

Fuente: Elaboración propia.

Identificar a alguien implica reconocer cualquier elemento que permita determinar la identidad del sujeto que realiza una acción. La continua utilización de los medios digitales para realizar actividades e interactuar con otras personas y entidades dan a la identidad digital un papel cada vez más relevante. Esta identidad digital está formada por diferentes tipos de datos que amplían de forma importante el contenido que posee la identidad física. En concreto, el tipo de datos que ayudan a configurar la identidad digital pueden catalogarse como:

- *Datos de identidad individual:* se refiere a identificadores como el nombre, el número de la seguridad social o el DNI, el número de la licencia de conducción, el número de la tarjeta de crédito, la fecha de nacimiento, los identificadores de los servicios que tiene contratados, etc.
- *Datos de comportamiento:* datos sobre transacciones, historial de navegación, datos de localización, transcripciones del *call center*, historial de compra, accesos, etc.
- *Datos derivados o calculados:* son atributos modelados de manera analítica que sirven para hacer un perfilado de las personas, por ejemplo, para valorar el riesgo de un cliente a la hora de darle un crédito, entender la propensión a hacer algo, valorar su influencia en un ámbito determinado, etc.
- *Datos que va creando el propio usuario de forma voluntaria al utilizar los servicios:* datos como opiniones sobre productos, redes profesionales a las que pertenece, «me gusta» en redes sociales, intenciones de compra, valoraciones y revisiones de productos, respuestas en foros, etc.

El concepto de identidad digital tiene diversos alcances en diferentes entornos, es decir, las personas cuentan con perfiles adaptados al contexto en el que se desenvuelven, y que incluyen distinta información. Por ejemplo, la información que necesita un centro médico sobre un paciente cuando ingresa por una dolencia es diferente de la información que requiere una

tienda para que pueda dar por válida una compra, o de la información que tienen los amigos sobre una determinada persona. Por tanto, la formulación de esta identidad depende en gran medida del entorno en el que se va a utilizar. Así podemos distinguir en una primera clasificación el entorno público del entorno corporativo y el de las aplicaciones sociales.

- *En el sector público* es fundamental la validación entre la identidad digital y la identidad física. Una identidad que guarda la relación uno a uno y que requiere una gran fiabilidad a la hora de comprobar que un usuario es quien dice que es. Por ese motivo, todo el proceso de alta de usuario requiere de un control estricto que asegure que un sujeto sea quien dice ser, incluyendo en ocasiones la presencia física en las instalaciones de la Administración y la entrega de documentos oficiales como el DNI. Una vez que un usuario está dado de alta, los requisitos para autenticarse en el sistema se reducen a poseer ciertos certificados o mostrar una información que en teoría solo debe tener la persona que se está tratando de autenticar, como información enviada al móvil o un dato determinado (por ejemplo, el resultado de una determinada casilla en la declaración de la renta del año anterior). El nivel de seguridad es variable dependiendo del servicio y de los métodos de validación utilizados.
- *Las corporaciones*, a la hora de relacionarse con otros usuarios, ya sean personas físicas o jurídicas, utilizan sus propias credenciales. Es necesario validar además una serie de atributos que, junto con la identidad física, vienen a construir un concepto más amplio que denominamos identidad corporativa, y generalmente se delega la responsabilidad de realizar las identificaciones a terceras entidades. Existe entonces un proceso de delegación de la validación de identidades; por ejemplo, la entidad bancaria se encarga de validar que un usuario es quien dice ser a la hora de abrir una cuenta, mientras que este mismo dato no es validado por una empresa que ofrezca un servicio comercial online. Un modelo de relación en el que los usuarios se convierten en clientes y que lleva a que la identidad digital adquiera otros atributos complementarios, además de los propios de la identidad física. Dado que muchos de estos aspectos son validados por terceras entidades, el nivel de seguridad dependerá en cada caso del nivel de seguridad de las entidades certificadoras. Es un modelo de identidad digital que no sigue la regla uno a uno con respecto a la identidad física; por ejemplo, una persona puede tener varias identidades, una por cada cuenta bancaria, en un servicio que para darse de alta requiera una cuenta bancaria.
- *Las redes sociales y otros medios sociales* no son rigurosos a la hora de garantizar una trazabilidad con la identidad física. De hecho, en la mayoría se pide que se introduzcan datos personales y otros atributos, pero no existe un proceso robusto de comprobación de dichos datos. El modelo de comprobación de la identidad suele consistir en utilizar como identificador los datos de otro servicio digital; por ejemplo, una cuenta de correo, con lo que se traspasa el problema de identidad a otro servicio que tampoco tiene un sistema robusto de comprobación. Al igual que en el caso anterior, no existe una relación uno a uno y generalmente una misma persona puede tener varias identidades en los servicios.

Los ciudadanos y empresas, ante la seguridad y privacidad

2.1 El internauta, ante la privacidad y la seguridad	10
2.2 La empresa, ante la privacidad y la seguridad	15

Durante los últimos años, la aparición de noticias sobre problemas relacionados con la privacidad que afectaban tanto a empresas como a personas, así como el robo de información personal o fotografías, ha despertado la conciencia en una parte muy importante de la sociedad respecto a la importancia que tiene proteger la información personal en Internet. Se trata además de una situación compleja, en la que el número y la variedad de ciberamenazas es cada vez más elevado dado el proceso de digitalización de toda la economía y el avance de nuevas tendencias tecnológicas, como la computación en la nube o el Internet de las cosas.

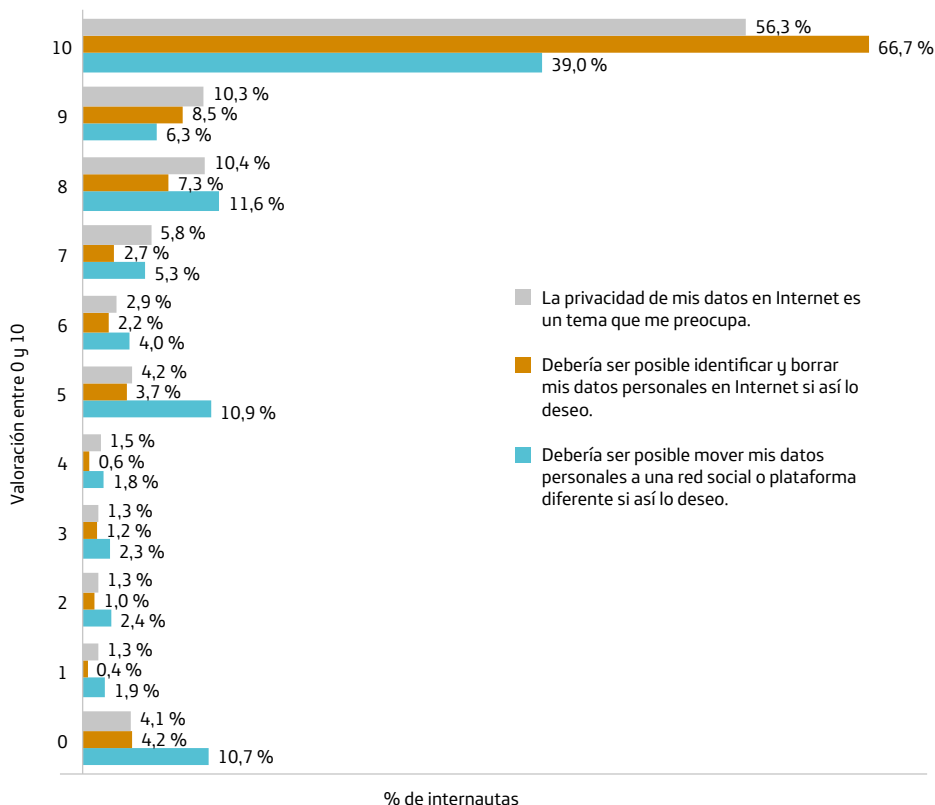
2.1 El internauta, ante la privacidad y la seguridad

Este proceso de digitalización de los servicios y de la economía en general implica importantes retos que conciernen a diferentes elementos del ecosistema digital. De entre los usuarios, las empresas suelen tener una mayor capacidad para afrontar estos retos, ya que disponen de más recursos y suelen contar con especialistas en tecnologías de la información, por ese motivo el internauta individual se puede considerar la parte más débil de este ecosistema. En esta sección analizamos la percepción de los usuarios ante la seguridad, las amenazas que se presentan hoy y las medidas que los usuarios toman ante esta situación.

2.1.1 Actitudes ante la privacidad

Esta situación en la que la seguridad y privacidad en Internet ha pasado a un primer plano ha llevado a Telefónica a realizar un estudio de campo para conocer la percepción de los usuarios ante estos temas. Según este estudio en el que los usuarios califican en una escala entre 0 y 10 su coincidencia con respecto a diferentes afirmaciones sobre privacidad, el 82,8 % reconoce este tema como de gran importancia (valoran este aspecto entre 7 y 10) y más de la mitad, el 56,3 %, lo valoran con 10, la máxima puntuación (tal y como se observa en la figura 2.1). También el 10 es la puntuación más común cuando se pregunta a los internautas acerca de si debería ser posible identificar y borrar los datos personales de Internet si así lo desea y si debería ser posible mover los datos a otra plataforma o red social, con un 66,7 % y un 39 % que muestran dicha calificación. Ampliando este rango a las calificaciones entre 7 y 10, que indican un sentir muy favorable con respecto al enunciado, observamos que estas cifras suben hasta el 85,2 % en el primer caso y al 62,2 % en el segundo.

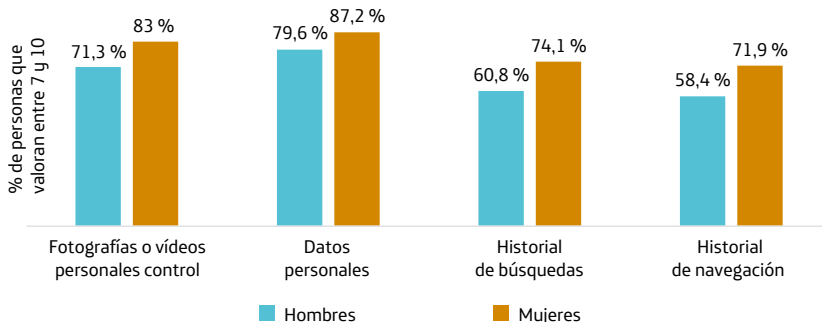
Figura 2.1 Percepción de los usuarios ante la seguridad y privacidad en Internet (valoración entre 0 y 10)



Fuente: Elaboración propia. Datos de Telefónica de 2015.

La información que los usuarios califican de personal y que no les gustaría que escapara de su control es muy variada, y se observa que las mujeres dan a la privacidad una mayor importancia (ver la figura 2.2). Así, al 71,3 % de los hombres y al 83 % de las mujeres les preocupa mucho que fotografías y vídeos personales escapen de su control (valoración entre 7 y 10); al 79,6 % de los hombres y el 87,2 % de las mujeres que se escapen datos personales; al 60,8 % de los hombres y al 74,1 % de las mujeres que lo haga el historial de búsquedas; y al 58,4 % de los hombres y al 71,9 % de las mujeres, el historial de navegación. Una diferencia de más de 10 puntos porcentuales para la mayoría de los tipos de información a favor de las mujeres que refleja su mayor preocupación. Un comportamiento que también se observa en las familias que tienen hijos pequeños y que muestra que también poseen una sensibilidad especial con todos los aspectos relacionados con la privacidad.

Figura 2.2 Preocupación por la privacidad según el tipo de información

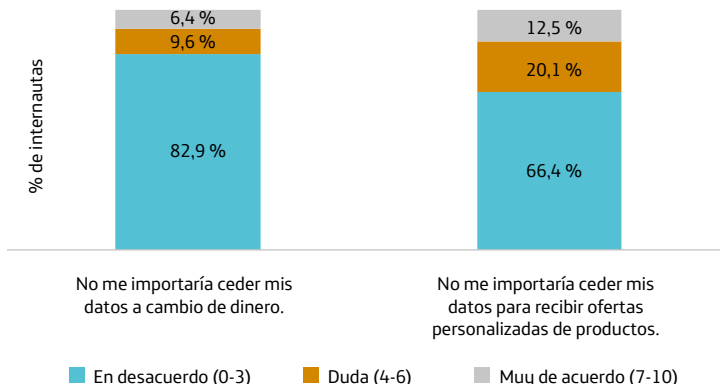


Fuente: Elaboración propia. Datos de Telefónica de 2015.

2.1.2 Actitudes ante la cesión de datos personales para obtener beneficios

En la actualidad existe un debate sobre la posibilidad de ceder datos personales a cambio de beneficios, ya sean en forma de dinero o mediante ofertas personalizadas de productos. De esta forma, el usuario se puede plantear ceder sus datos a cambio de recibir parte de los beneficios que las empresas consiguen por el uso de dichos datos. A pesar de que la idea parece positiva para los intereses de los usuarios, más aún cuando en la actualidad la mayoría cede sus datos sin recibir ningún tipo de compensación por ello, estas cifras muestran que la mayoría de la población no está de acuerdo con ceder parte de la privacidad a cambio de ofertas personalizadas o dinero. Así, solamente un 12,5 % está muy de acuerdo con ceder sus datos a cambio de recibir ofertas personalizadas, un 8,5 % en caso de familias con niños pequeños; y un 6,4 % los cederían por dinero, un 3,3 % entre 35 y 44 años, y el 5,7 % mujeres.

Figura 2.3 Interés por ceder datos a cambio de beneficios



Fuente: Elaboración propia. Datos de Telefónica de 2015.

2.1.3 Ciberamenazas a la privacidad de los usuarios

Los usuarios presentan una actitud de preocupación e interés ante estos temas, aunque, según se mostrará más adelante, en muchas ocasiones no son capaces de identificar cuáles son los peligros y por tanto no saben cómo enfrentarse a ellos. Una primera medida en este sentido será el conocer cómo el *malware* llega hasta nuestros sistemas, que deberá condicionar nuestro comportamiento; por ejemplo, no seguir cadenas de correos, utilizar *software* de fuentes seguras, tener cuidado al introducir USB de terceras personas... y es que los medios de distribución de *software* dañino son cada vez más variados.

A esta situación ha de añadirse que la naturaleza y los objetivos de los ataques cibernéticos han ido cambiando con el tiempo. Por ejemplo, la mayoría de los usuarios piensa que los atacantes van a ir detrás de información suya, ya sea personal o claves. No obstante, en muchas ocasiones, el objetivo de los atacantes es acceder a los recursos del usuario, como aprovechar el poder de procesamiento para realizar tareas que requieran gran poder de computación, como realizar *bitcoin mining*. Otro ejemplo sería el de acceder a su ancho de banda para que su sistema actúe como un zombi dentro de una *botnet* y poder realizar ataques masivos.

Es posible que el usuario considere que no tiene ninguna información relevante que pueda ser utilizada por delincuentes. Eso suele ser una percepción falsa, ya que los atacantes pueden querer acceder a las libretas de contactos para realizar spam masivo personalizado y atacar a terceras personas, o bloquear el ordenador y pedir un rescate por recuperar la información, pues aunque la información no sea de valor para terceras personas, sí lo será para el propio usuario.

Los robos más importantes de información pueden afectar a tres tipos de aspectos:

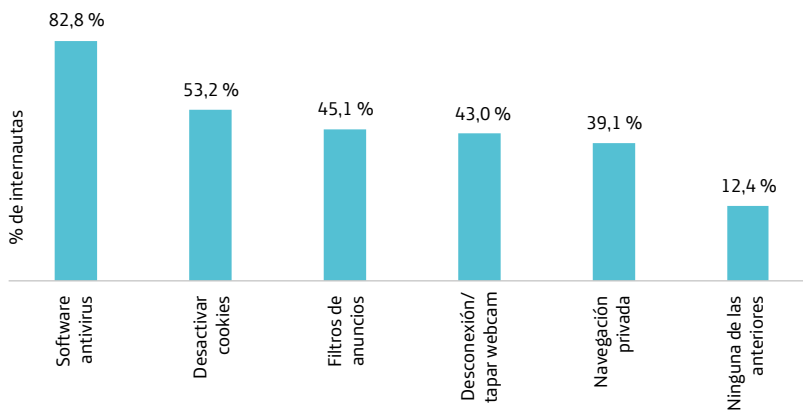
- **Económico:** si te roban las contraseñas o tienen acceso a sistemas online como bancos, Paypal, bitcoins...
- **Lúdico:** se refiere a la pérdida de fotografías, acceso a información sensible como repositorios en la nube...
- **De «imagen»:** si roban cuentas de las redes sociales, pueden llegar a suplantar la identidad y dañarla.

Es necesario que los usuarios sean conscientes de las nuevas normas de juego que imponen Internet y las nuevas tecnologías y conozcan tanto los mecanismos más importantes que utilizan los atacantes como cuáles de nuestras identidades pueden ser interesantes para ellos.

2.1.4 Medidas relacionadas con privacidad y seguridad tomadas por los usuarios

Esta situación muestra cómo el número y las características de las amenazas han ido evolucionando con respecto a hace unos años, cuando Internet no era tan habitual y además no existían tecnologías como la computación en la nube o los *smartphones*. Se observa que el entorno tecnológico ha cambiado sustancialmente en los últimos años, la digitalización ha llegado a prácticamente todos los servicios y se ha pasado de una comunicación esporádica a estar continuamente conectados con el entorno. Se trata pues de una situación completamente diferente a la que existía hace unos años, y que debería suponer una transformación completa de las medidas y actitudes que los usuarios tomaran en referencia a la privacidad y seguridad en su mundo digital. No obstante, según se desprende de la encuesta de hábitos realizada por Telefónica, estas nuevas circunstancias no están siendo interiorizadas por los usuarios, que en su mayoría siguen confiando en los antivirus como fórmula preferida para proteger su privacidad. Se observa que la mayoría de estas medidas delegan la protección de su privacidad en poseer *software* especializado, como antivirus o filtros de anuncios, en vez de medidas activas como cambios en los hábitos. La excepción más reseñable de comportamiento activo con respecto a la seguridad es desconectar o tapar la webcam, hábito que llega al 43 % de los internautas y alcanza al 45,7 % en el caso de las mujeres y el 54,4 % entre los jóvenes entre 20 y 24 años.

Figura 2.4 Medidas para proteger la privacidad tomadas por los internautas



Fuente: Elaboración propia. Datos de Telefónica de 2015.

Se deduce que existe una cierta inercia en los comportamientos con respecto a la seguridad y que todavía la mayoría de la población internauta mantiene los hábitos que tenía en la época en que la conexión a Internet era más puntual y las tecnologías estaban más restringidas a actividades muy concretas. Se hace imprescindible una actividad de concienciación y formación sobre los peligros y qué comportamientos podrían evitarlos.

2.2 La empresa, ante la privacidad y la seguridad

El problema de la privacidad y la seguridad en el entorno empresarial tiene muchas similitudes con el usuario individual. No obstante, lo que en un caso puede suponer la pérdida de unas fotos que tienen un gran valor sentimental, en el de una empresa puede representar que la organización no pueda desarrollar su trabajo porque los sistemas no funcionan o incluso la pérdida de información comercial importante y, en última instancia, espionaje industrial. Por estos motivos, las empresas suelen tener una concienciación mayor ante este tipo de situaciones.

2.2.1 Ciberamenazas a la privacidad y seguridad de las empresas

Al igual que en el apartado anterior, no nos extenderemos en los distintos tipos de amenazas, puesto que es el tema de este monográfico y se tratará de una u otra forma a lo largo de él. Sí que merece la pena mencionar que se pueden diferenciar claramente entre dos tipos de amenazas diferentes:

- Ataques a su red privada (ordenadores donde trabajan sus empleados)
- Ataques a su infraestructura (servidores, redes, repositorios de ficheros, etc.)

Podemos hablar en los mismos términos que el usuario. Sin embargo, como se ha comentado, el efecto es diferente: si ante un problema de *ransomware* (tipo de programa informático malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado y pide un rescate a cambio de quitar esta restricción) un usuario en casa pierde las fotos del fin de semana en el campo, en una empresa puede perder la facturación de un año, y con ella, clientes.

Si el ataque se dirige a la infraestructura, los problemas pueden ser espionaje o robo de información. También, si acceden por ejemplo a las redes sociales, pueden dañar la imagen. Si bien es cierto que las redes sociales forman parte de la infraestructura, están gestionadas al fin y al cabo por una persona sentada frente a un ordenador en la oficina, y el objetivo también puede ser esa persona. Para ello pueden acceder a su sistema o de alguna manera (ingeniería social) obtener sus contraseñas.

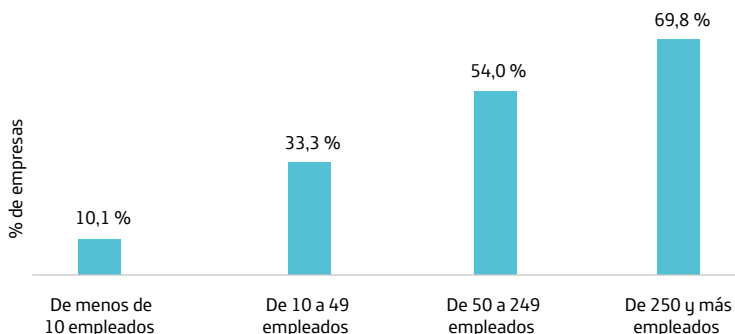
Otro tipo de amenaza son las amenazas persistentes avanzadas, también conocidas por sus siglas en inglés, APT (por *Advanced Persistent Threat*), todo un conjunto de procesos informáticos que se llevan a cabo generalmente de manera sigilosa y continua. Suelen estar orquestados por personas y se dirigen a romper la seguridad de un entidad determinada. Este tipo de entidades suelen ser empresas, organizaciones o naciones, y generalmente se llevan a cabo por motivos de carácter político. Este proceso tiene una naturaleza avanzada, pues involucra sofisticadas técnicas que emplean *software* malicioso para explotar vulnerabilidades en los sistemas.

2.2.2 Medidas relacionadas con privacidad y seguridad tomadas por los usuarios

Como se ha comentado, los ciberataques sobre las empresas tienen generalmente un impacto, al menos económico, superior a cuando se producen sobre las personas. Por ese motivo las empresas suelen definir planes relativos a la seguridad tecnológica. No obstante, las empresas más pequeñas tienen más dificultad a la hora de poner en marcha estos planes, ya que disponen de menos recursos y formación específica en este tipo de tecnologías. Según se muestra en la figura 2.5, en el caso de las empresas de menos de 10 empleados, tan solo una de cada diez ha definido una política de seguridad.

Si bien es cierto que a medida que las empresas tienen mayor dimensión, el número de ellas que tienen definido este tipo de políticas crece, no deja de llamarnos la atención que más del 30 % de las empresas de más de 250 empleados y casi la mitad de entre 50 y 249 no tengan ningún tipo de política de seguridad definida.

Figura 2.5 Empresas con política de seguridad definida



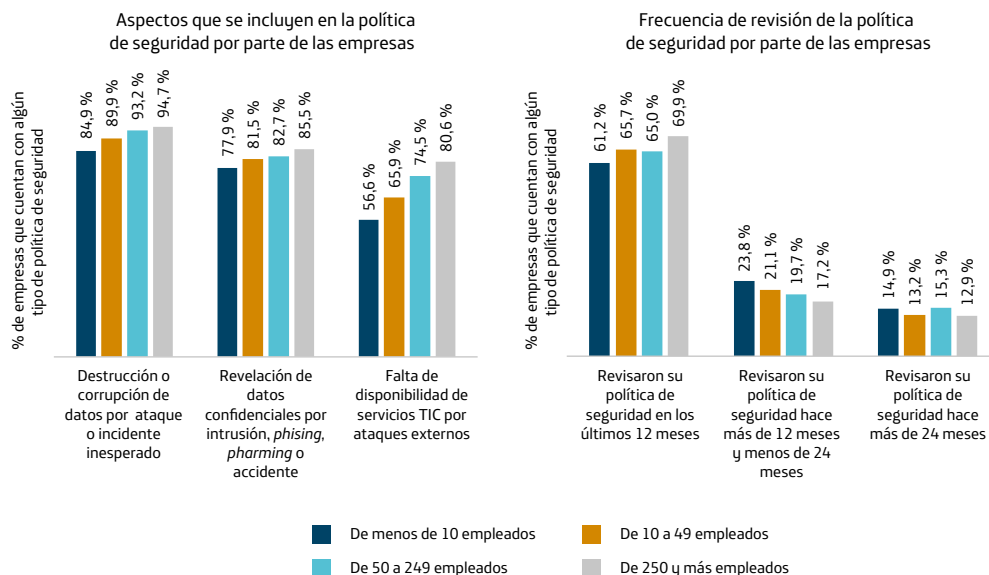
Fuente: INE. Datos de 2015.

Estos datos nos muestran que todavía existe una gran labor por realizar a la hora de concienciar a las empresas sobre la importancia de la seguridad y cómo en un entorno como el actual no se puede confiar toda la protección a tener un *software* instalado como antivirus, sino que es necesario un planteamiento y unas políticas globales.

De entre las empresas que disponen de este tipo de políticas de seguridad, se observa que ya no existe una brecha tan importante entre ellas en función del tamaño, aunque se sigue dando el caso de que las empresas cuanto más grandes, más aspectos tienen en cuenta en los planes de seguridad, además de realizar revisiones de dichos planes con una frecuencia superior.

El principal peligro por el que las empresas se preocupan a la hora de tener en cuenta sus políticas de seguridad es evitar la destrucción de los datos que estas utilizan en su operación, aspecto que es tenido en consideración en un 94,7 %; seguido de la revelación de datos confidenciales, que es considerado por el 77,9 % de las empresas de menos de 10 empleados y por el 85,5 % de las empresas con más de 250 que tienen planes de seguridad. Respecto a la frecuencia con la que se revisan estas políticas, dos de cada tres empresas comprobaron los planes en los últimos doce meses y tan solo una baja porción de ellas lo hizo hace más de veinticuatro, lo que demuestra que existe un interés por actualizarse en aspectos relacionados con la seguridad. De nuevo se aprecia que las empresas de mayor tamaño realizan revisiones de estos planes con mayor frecuencia, posiblemente al disponer más habitualmente de empleados expertos en IT.

Figura 2.6 Medidas de seguridad por parte de las empresas



Fuente: INE. Datos de 2015.

El ciclo de vida de la ciberseguridad

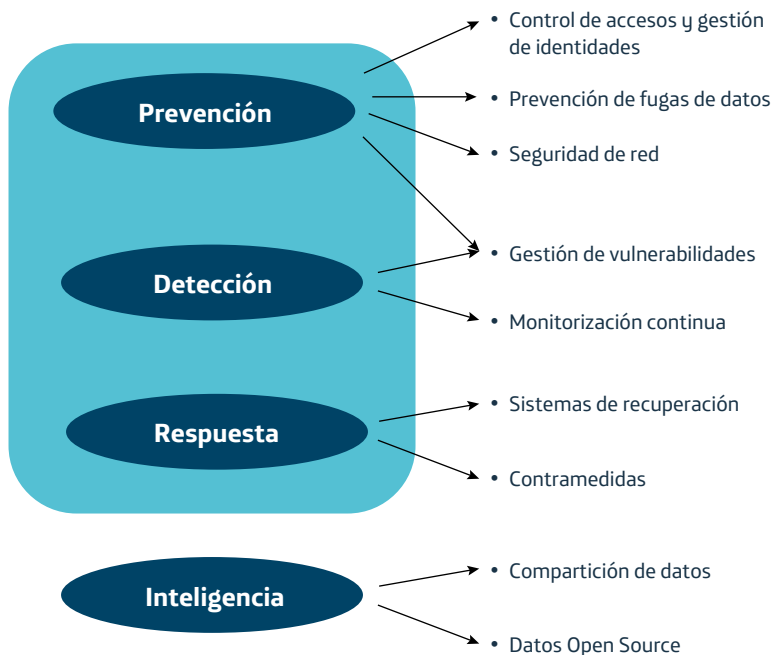
3.1	Prevención	21
3.2	Detección	28
3.3	Respuesta	30
3.4	La inteligencia para dotar de eficiencia a las medidas de ciberseguridad	35

Dentro del entorno tecnológico, la ciberseguridad debe ser considerada un proceso y no una actividad aislada y diferenciada del resto de los servicios o herramientas informáticas. En el mundo actual, digitalizado y en el que Internet es ya parte esencial de cualquier servicio, organización o entorno, la seguridad es una cualidad más que, como la salud en las personas, hay que cuidar desde el principio y en cuya gestión participa gran cantidad de agentes.

Siguiendo la comparación con la salud, los ciberataques se pueden equiparar a una enfermedad que debemos ser capaces de prevenir y ante la que debemos ser capaces de reaccionar, generando los anticuerpos necesarios para volver a la situación de salud inicial.

La ciberseguridad es, en este sentido, un proceso que implica prevención, detección y reacción o respuesta, y que debe incluir un elemento de aprendizaje para la mejora continua del propio proceso.

Figura 3.1 Etapas en la gestión de la ciberseguridad



Fuente: Elaboración propia.

Dado el carácter global que tienen actualmente los servicios tecnológicos, y en consecuencia también las amenazas, cada vez es más necesario elaborar modelos de seguridad que tengan este mismo carácter global. Para que esto sea posible, es imprescindible dotar los sistemas de ciberseguridad de una inteligencia que permita este aprendizaje y que sea ca-

paz de integrar información de diferente naturaleza (ver la figura 3.1), por ejemplo de asociar diferentes señales que por separado no sean relevantes, pero que tenidas en cuenta de manera conjunta puedan identificar una amenaza global. De esta forma, al igual que sucede en otros campos, el compartir datos y el desarrollo de modelos *open source* se convierte en un factor decisivo para conseguir abordar el problema de una forma integral.

3.1 Prevención

Dentro del enfoque global que se ha mencionado anteriormente, la prevención ha de ser abordada por el usuario y la empresa desde varias perspectivas. Por un lado, es importante estar informado de la evolución de las amenazas, de las posibles estafas y de qué soluciones existen contra ellas. Por ello, la formación constante es un elemento esencial en la prevención. Es recomendable adquirir una serie de conocimientos sobre seguridad que son necesarios poner en marcha con una actitud de prudencia y utilizar con la mayor eficacia y eficiencia posibles todos los medios a nuestro alcance. Por otro lado, es necesario conocer el funcionamiento de las herramientas o productos de seguridad, sus características y su forma de actuar para sacarle el mayor partido posible y conseguir la protección más efectiva. También es necesaria la protección física de las instalaciones para garantizar que nadie sin autorización pueda manipular los terminales, los accesos a la red o conectar dispositivos no autorizados³.

Como puede verse en el gráfico anterior, la prevención tiene tres procesos críticos: control de accesos y gestión de identidades, prevención de fugas de datos y seguridad de la red. Brevemente se describirán cada uno de estos procesos.

3.1.1 Control de accesos y gestión de identidades

Dos procesos importantes para la ciberseguridad en una empresa son el control de accesos y la gestión de identidades. Estos dos conceptos, aunque diferentes, se dan la mano el uno con el otro para desarrollar sus funciones, que son básicamente controlar los accesos a los sistemas, tanto físicos como informáticos.

La gestión de identidades es un proceso relevante a la hora de prevenir ataques, ya que consiste en asignar a una identidad concreta un rol o una serie de permisos o credenciales para acceder a ciertos sistemas o recursos, especialmente a las aplicaciones críticas y zonas restringidas. En todas las organizaciones existen zonas donde se almacena información confidencial o de suma importancia. Por eso es recomendable implementar una serie de políticas de control sobre quiénes podrán acceder a los activos críticos para minimizar el riesgo, y esto se realiza mediante las herramientas que nos ofrecen el control de accesos y la gestión de identidades.

3. «Taxonomía de soluciones de ciberseguridad 2015», Incibe.

Para la correcta gestión de los controles y las identidades, es necesario llevar a cabo acciones de inventariado y catalogado y establecer los criterios de acceso. Estos criterios de acceso deben regirse por la máxima de que una persona debe tener disponibilidad de las aplicaciones críticas o zona restringida solo cuando el ejercicio de su trabajo lo requiera⁴.

En numerosas ocasiones, la gestión de identidades, y por tanto el control de accesos, es llevada a cabo mediante procedimientos manuales. Sin embargo, los expertos en el ámbito de la gestión de identidades advierten de que uno de los principales problemas que acarrear los procesos manuales en este ámbito es su ineficiencia⁵. Adicionalmente a este problema los principales retos que la gestión de identidades plantea a las organizaciones son la previsión, la gestión de cuentas huérfanas y la adaptación a la normativa vigente.

El primer gran reto es poseer en las organizaciones un sistema organizado de previsión, de modo que cada persona tenga sus credenciales en tiempo y forma. Adoptando sistemas de previsión se evitarían muchos problemas de seguridad, especialmente cuando existen cambios de roles dentro de una organización; como que una persona con el rol equivocado acceda a funciones o zonas para las que no está autorizada. Por eso es necesario ser ágil a la hora de realizar estos cambios y hay que tener un protocolo eficaz para asignar las claves y los usuarios que cada rol requiera. El segundo reto de la gestión de identidades es lo que se da en llamar las cuentas huérfanas. En muchos casos, una persona deja una organización y hay que gestionar que la cuenta de ese trabajador quede totalmente anulada. El problema es que en numerosas ocasiones el trabajador es dado de baja en aquellos aspectos que se encuentran reglados en el protocolo interno de la empresa, pero puede que existan aspectos ligados a la seguridad que estén siendo gestionados por un tercero; por ejemplo, el control de los tornos de entrada en un edificio, y que no están contemplados en el protocolo interno, por lo que su gestión es más lenta. Por último, el gran reto en cuanto a la gestión de identidades es el de las normativas de seguridad aplicables. Estas cada vez son más exigentes con las organizaciones y, a medida que una organización crece, tiene que cumplir más requisitos. Por eso es importante trabajar en la utilización de contraseñas más fuertes, poder resetear estas cuando se ha detectado un ataque y ser capaces de detectar de forma proactiva patrones de comportamiento en el ámbito de la seguridad que se salen de lo normal para poder actuar antes de que un ataque o una amenaza se produzca⁶.

Para resolver estos problemas que se han mencionado, en el nivel más básico, es necesario que este proceso se encargue de definir qué usuarios pueden hacer determinadas acciones y en qué circunstancias o requisitos. Para ello, las herramientas de gestión de identidades, en empresas u organizaciones de cierta entidad y volumen de negocio, suelen ser gestionadas mediante servidores dedicados exclusivamente a esta función, en busca de incrementar

4. «Buenas prácticas en el área de informática», Incibe.

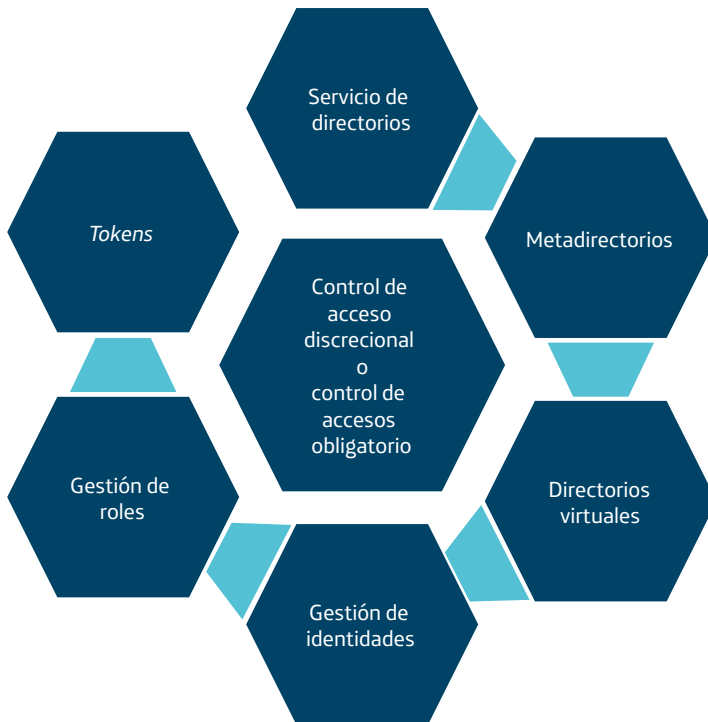
5. <http://globssecurity.com/en-gestion-de-identidades-no-se-puede-hacer-lo-de-siempre-ignacio-gilart-wbso-32151/>

6. *Ibidem*.

la seguridad del proceso. En el núcleo de la gestión de identidades se establecen los requisitos por los que un determinado usuario podrá realizar unas acciones u otras, en qué ubicaciones lo podrá hacer y en qué circunstancias. Esto también dependerá de establecer una administración adecuada que incluya una definición clara de políticas, de elaboración de informes, alertas y requisitos de gestión común de operaciones.

Los principales componentes que suelen encontrarse en una solución de gestión de identidades son: el servicio de directorios, los metadirectorios, los directorios virtuales, la gestión de identidades, la gestión de roles, los *tokens*, el control de acceso discrecional y el control de acceso obligatorio⁷.

Figura 3.2 Componentes de una solución de gestión de identidades



Fuente: Elaboración propia a partir de datos de USBMed.

El servicio de directorios se puede definir como un componente de la red que permite la administración de un directorio de forma centralizada, al mismo tiempo que provee informa-

7. José A. Montoya S. y Zuleima Restrepo R., «Gestión de identidades y control de acceso desde una perspectiva organizacional», Ing. USBMed, vol. 3, núm. 1, enero-junio 2012.

ción para las aplicaciones organizacionales que interactúan con él. Otra característica propia es que no solo permite almacenar usuarios, también almacenar recursos que pueden ser útiles para el negocio.

Los *metadirectorios* son un servicio de directorio que posibilita recolectar y almacenar información de varios servidores de directorios. Algunos de estos metadirectorios, además, tienen la capacidad de integrar información disponible en bases de datos y en su consolidación puede ser transformada según las reglas que se tengan definidas en él para los procesos de recolección e importación de los datos. Pero su principal característica y ventaja es que permiten a la organización que lo está utilizando integrar en un único repositorio la información almacenada y proveniente de diferentes fuentes.

En cuanto a los *directorios virtuales*, tienen funciones similares a las de los metadirectorios. Se encargan de crear una visión unificada de la información que procede de las diferentes fuentes con las que cuenta la organización. Pero aunque el concepto es similar, también existen una serie de diferencias importantes. La principal es que el directorio virtual no utiliza a los agentes para la recolección de datos; por el contrario, se encarga de crear una vista única por medio del mapeo de campos en un esquema virtual. Por tanto, poseen más flexibilidad, debido a que no tienen que realizar el almacenamiento de los datos en un repositorio central, con lo que se elimina la necesidad de tener que desarrollar procesos de sincronización y replicación de datos entre servicios de directorios.

La gestión de identidades, valga la redundancia, es uno de los servicios más importantes dentro del *Identity Management*. Como se ha comentado anteriormente, en las empresas actualmente se trabaja con un gran número de aplicaciones y sistemas que son utilizados por diferentes personas para la realización de las tareas que sus cargos conllevan. Todas estas aplicaciones y sistemas, por lo general, manejan sus repositorios propios con la información de las cuentas de los usuarios. Esto hace que existan múltiples cuentas y múltiples contraseñas para un mismo usuario en las diferentes aplicaciones. Por ello, la gestión de identidades permite gobernar la creación, desarrollo y eliminación de las entidades y sus atributos dentro de un repositorio unificado de identidades.

En la *gestión de roles* se tramita la vida de los roles asociados a los usuarios de la organización. Aquí se identifican dos tipos: los roles de negocio y los roles de aplicación. Los primeros establecen la posición jerárquica del usuario dentro del esquema de una organización; los segundos, los permisos sobre los recursos. Para vincular estos dos tipos de roles existen dos fórmulas. Por un lado está el modelo *top-down*, que va de lo general a lo particular, que provoca que los roles de negocio tengan inventariadas las funciones de cada aplicación a las que necesita acceder. Cada una de estas funcionalidades se encuentra relacionada con permisos, que a su vez están asociados a roles de aplicación. Por otro, el *bottom-up*, que va de lo particular a lo general. Con este enfoque, el punto de partida se encuentra en los permisos que se necesitan para acceder a las funcionalidades de las aplicaciones o sistemas de la or-

ganización. Estos permisos van asociados a roles de aplicación que por medio del establecimiento de políticas bien definidas se vinculan a roles de negocio.

Dentro de los *tokens*, el uso de nombres de usuario y contraseñas es el mecanismo más común a la hora de autenticación de los usuarios. Este mecanismo ha tenido como resultado, en muchas ocasiones, la proliferación de cuentas debido al número de aplicaciones que un usuario necesita utilizar para poder trabajar.

En un nivel superior de seguridad se encuentran los *certificados digitales*. Los certificados se basan en criptografía de llave pública, en la que una entidad se encarga de avalar la identidad del usuario contenido dentro del certificado digital. Cuentan con mayor complejidad a la hora de ser utilizados por el usuario final, que precisa de un conocimiento más avanzado que para otro tipo de mecanismos de seguridad, y deben ser renovados periódicamente.

Los *dispositivos biométricos* son los que se basan en el reconocimiento de características fisiológicas de cada persona. Por medio de estos dispositivos se pueden reconocer rasgos faciales, huellas, el iris, la geometría de una mano, etc. Estos dispositivos tienen la ventaja de que al estar basados en características propias del sujeto, su vulneración es más difícil. La problemática existente con este tipo de dispositivos es que hay personas que no se encuentran dentro del conjunto de los patrones estándares de reconocimiento de los dispositivos, por lo que este tipo de personas no los podrían utilizar.

El *control de acceso discrecional* consiste en un mecanismo restringido del acceso a recursos basado en la identidad del sujeto o del sujeto y de los grupos a los que pertenece. Con este método, existe la figura denominada «el custodio», que brinda la posibilidad de decidir a qué usuarios se les permite el acceso. Una vez que se ha otorgado este acceso a otros usuarios, la desventaja más importante es que no se puede tener una administración centralizada de los permisos de acceso a recursos al depender del usuario.

Por último, existe el *control de acceso obligatorio*, con el que el dueño de la información es el que define la política, y los custodios y usuarios están obligados a cumplirla. Con este modelo, los usuarios no pueden sobrescribir o modificar la política⁸.

3.1.2 Prevención de fugas de datos

La fuga de datos es uno de los principales problemas de seguridad y uno de los retos a los que se enfrentan usuarios, empresas y organizaciones. Ejemplos de esta amenaza los encontramos en la fuga de datos que sufrió eBay y que pudo afectar a un total de 128 millones

8. *Ibidem*.

de usuarios⁹, o la que experimentó el Gobierno de Estados Unidos en junio de 2015, que se estima que afectó a 4 millones de empleados de la Administración federal¹⁰.

Los incidentes de este tipo son complejos debido a la diversidad y a las graves consecuencias que pueden acarrear. Muchas de las fugas de datos tienen un componente humano y organizativo.

Para afrontar este reto, empresas y organizaciones cuentan con una amplia oferta de herramientas y medidas que de una forma eficaz ayudan a minimizar y prevenir la temida fuga de datos. Estas medidas y herramientas se pueden agrupar en tres grupos diferentes. En el primer grupo se englobarían todas las medidas técnicas; en el segundo, las de carácter organizativo, y en el tercero, las medidas legales.

Entre las medidas técnicas se hallan: control de acceso e identidad, soluciones *antimalware* y antifraude, seguridad perimetral y protección de las comunicaciones, control de contenidos y control de tráfico, copias de seguridad, control de acceso a los recursos, actualizaciones de seguridad y parches y, por último, otras medidas de seguridad derivadas del cumplimiento de legislación, gestión de eventos e inteligencia de seguridad.

En cuanto al ámbito organizativo, las actuaciones que se pueden desarrollar son: establecer un código de buenas prácticas, una política de seguridad, procedimientos de clasificación de la información, establecimiento de roles y niveles de acceso, formación e información interna y sistemas de gestión de seguridad de la información.

Legalmente se pueden tomar las siguientes medidas: solicitud de aceptación de política de seguridad, solicitud de aceptación de política de confidencialidad, medidas de carácter disuasorio atendiendo a la legislación y relativas a la adecuación y cumplimiento de la legislación aplicable (LOPD, LSSI, etc.)¹¹.

Un modelo de estrategia, para afrontar de forma eficaz la prevención de fuga de datos de una forma holística y que engloba tanto medidas técnicas como organizativas y legales, es lo que se conoce como *Data Leak Prevention*, *Data Loss Prevention* o *Extrusion Prevention*. Con él se pretende asegurar que no se puede extraer información sensible o crítica fuera de la red de una corporación. También se utiliza este término para describir tipos de *software* con los que el administrador de una red puede controlar la información que los usuarios de dicha red pueden transmitir. Con estos productos *software* se establecen reglas de negocio con las que se clasifica y protege la información para que el personal que no se encuentra autorizado no pueda, tanto accidental como voluntariamente, enviarlos fuera de la organización y ponerla

9. https://www.incibe.es/technologyForecastingSearch/CERT/Alerta_Temprana/Bitacora_de_ciberseguridad/Intrusion_eBay

10. https://www.incibe.es/technologyForecastingSearch/CERT/Alerta_Temprana/Bitacora_de_ciberseguridad/fuga_informacion_US

11. «Guía gestión de fuga de información», Incibe.

en riesgo. Este *software* suele incluir gran cantidad de políticas predefinidas, que permiten también la definición de políticas personalizadas de acuerdo con las demandas concretas de cada compañía¹².

Hay varios motivos por los que el DLP es más seguro que otras tecnologías como los cortafuegos y los IDS (*Intrusion Detection Systems*) o IPS (*Intrusion Prevention Systems*). La principal diferencia es que esta tecnología identifica los datos y el contenido sensible conforme a unas reglas que se han establecido previamente¹³.

También contribuye a mejorar el seguimiento de los protocolos que ha suscrito una empresa. En muchas ocasiones, sobre el papel, parece que estos protocolos se están siguiendo correctamente. Pero es solo cuando se establecen dispositivos de control y prevención cuando verdaderamente se puede descubrir si los protocolos son suficientes o no. Con este tipo de medidas y de *software* se pueden reducir de forma mucho más efectiva las fugas de datos¹⁴.

Cuando una empresa está dispuesta a adoptar una política de estas características con la que protegerse de posibles fugas de datos sensibles que puedan suponer un grave riesgo para la integridad de su organización, para su modelo de negocio, su estrategia de ventas u otra política estratégica de similares características, la primera premisa que ha de tenerse en cuenta es cuáles son sus necesidades y qué soluciones podrían resultar más satisfactorias para resolverlas. Después de tener claro este supuesto, es aconsejable priorizar sistemas DLP que nos ofrezcan monitorización continua, una gestión centralizada, más sencilla de llevar a cabo que una descentralizada, que establezcan requisitos claros a la hora de realizar copias de seguridad y almacenamiento, que sea fácil de integrar en los sistemas corporativos, con prestaciones adicionales y conocida en el mercado¹⁵.

3.1.3 Seguridad de red

La seguridad de red hace referencia a todas aquellas acciones encaminadas y diseñadas para proteger una red de sistemas u ordenadores y recursos de acceso de red. Esencialmente estas actividades se encaminan a proteger el uso de las redes, el grado de fiabilidad, la integridad y la seguridad de las redes y de los datos que se transmiten a través de ellas. Una seguridad efectiva de la red se dirige a la protección de una amplia variedad de amenazas y a evitar su entrada en la red o que se expanda por ella, por lo que es un elemento esencial de una correcta política de prevención en materia de ciberseguridad.

12. <http://whatis.techtarget.com/definition/data-loss-prevention-DLP>

13. Prathaben Kanagasingham, «Data Loss Prevention», SANS Institute InfoSec Reading Room.

14. «Guía gestión de fuga de información», Incibe.

15. *Ibidem*.

Para proteger nuestra red de virus, troyanos, espías, hackers, robos de identidades, etc., es necesario contar con varias capas de seguridad para que si una falla, la otra actúe y lo detenga. En este sentido se refiere a una estructura en forma de anillos o capas, similar al concepto que ya se ha comentado en los sistemas operativos de confianza.

En cuanto a la seguridad de la red, será necesario implementar medidas de seguridad tanto de *hardware* como de *software*. Este último, además, requerirá una actualización constante, lo que reducirá las posibilidades de verse afectados por una amenaza. Los principales componentes que normalmente incluye esta política de seguridad en el apartado del *software* son el antivirus y el antispyware y los cortafuegos con los que bloquear accesos no autorizados a nuestra red. Existen además sistemas que analizan constantemente datos sobre el uso de las redes y que pueden ayudar a detectar intrusos a través de la detección de anomalías en estos usos. En referencia al *hardware*, las medidas suelen estar encaminadas al control de acceso mediante sistemas de autenticación, como por ejemplo los de tipo biométrico que ya se han mencionado o los *token* de seguridad.

Una política de seguridad de la red debe incluir tres pasos fundamentales, comunes a cualquier política de seguridad: la definición de una política de seguridad clara sobre nuestra red, su implementación y su continua auditoría.

3.2 Detección

En el campo de la ciberseguridad, otro proceso destacado es la detección de incidencias. La detección puede ocurrir mientras se está produciendo el ataque o pasado un tiempo desde el mismo.

La detección de un ataque o amenaza en tiempo real suele producirse gracias a la detección del *malware* por parte de un antivirus. Si por el contrario se da la segunda circunstancia, los problemas son mayores porque los hackers han podido actuar libremente durante un largo período de tiempo. Se estima que el período medio entre el momento en que se produce una brecha de seguridad y su detección fue en 2014 de 205 días¹⁶.

Afortunadamente, se puede afirmar que las herramientas de ciberseguridad existentes en la actualidad realizan de forma eficaz la detección de patrones de ataque conocidos si se encuentran instaladas correctamente. El problema lo encontramos con los ataques con patrones desconocidos y cuando la detección no se ha producido en tiempo real y ha pasado un período largo hasta que finalmente se produce la detección. Esto se ha convertido en un problema creciente porque la forma de actuar de los hackers ha cambiado notablemente en los últimos años. Se ha pasado de un modelo de ataques con patrones más reconocibles,

16. «M-Trends 2015: «A view from the front lines; Threat Report», Mandiant.

en momentos concretos y determinados, a un modelo de ataques diversificados que se pueden producir en cualquier momento¹⁷. Por eso la detección proactiva se está convirtiendo en un elemento muy relevante para asegurar la seguridad de los sistemas. Este modelo, a diferencia del reactivo, permite una detección de las amenazas temprana y consigue que los problemas que puedan surgir se solucionen de una forma más eficiente¹⁸. Con este modelo no solo se utilizan las defensas habituales, sino que se combinan junto con otras diferentes que, cada cierto tiempo, se utilizan con una configuración más agresiva. También resulta interesante realizar una revisión periódica de la red, aunque implique una inversión de tiempo y una ralentización de la producción de la organización.

Los dos aspectos más importantes a la hora de actuar en la detección de amenazas y ciberataques son, como se apreciaba en la figura 3.1, la gestión de vulnerabilidades y la monitorización continua. Ambos son fundamentales para una correcta detección y el uno se engloba dentro del otro. Así, dentro del plan de gestión de vulnerabilidades es necesario contemplar una monitorización continua de los sistemas informáticos de la empresa u organización. La gestión de vulnerabilidades permite obtener una visión continua de las flaquezas y debilidades en el entorno de las TI y de los riesgos que se le asocian. Solamente identificándolos y mitigándolos una organización puede prevenir los ataques que pretendan penetrar en las redes de una empresa u organización y robar información.

Es importante no confundir la gestión de vulnerabilidades con el escaneo de vulnerabilidades. Las dos se encuentran relacionadas, pero la segunda consiste en la utilización de un programa informático con el que se identifican los puntos débiles de nuestra red, la infraestructura informática o las aplicaciones. La primera es el proceso que engloba la búsqueda de estos puntos débiles, y que tiene en cuenta otros aspectos como los riesgos que pueden ser aceptados o las soluciones que van a requerir un riesgo determinado. Por ello, su objetivo principal es detectar y solucionar las debilidades de manera oportuna.

El principal problema surge cuando las empresas u organizaciones no realizan búsquedas (o escaneo) de potenciales vulnerabilidades en sus sistemas de forma habitual. En muchos casos estas acciones se realizan trimestral o anualmente, lo que solo muestra la realidad de la infraestructura en ese momento determinado. Por eso, dentro del plan de gestión se ha de incluir un sistema de monitorización continua y frecuente. De lo contrario, cualquier problema no detectado después del escáner realizado no se conocerá hasta el próximo y puede dejar los sistemas en peligro durante un largo período de tiempo. De este modo, para detectar las amenazas de forma eficaz, es necesario un plan de monitorización continua de los riesgos y las vulnerabilidades¹⁹.

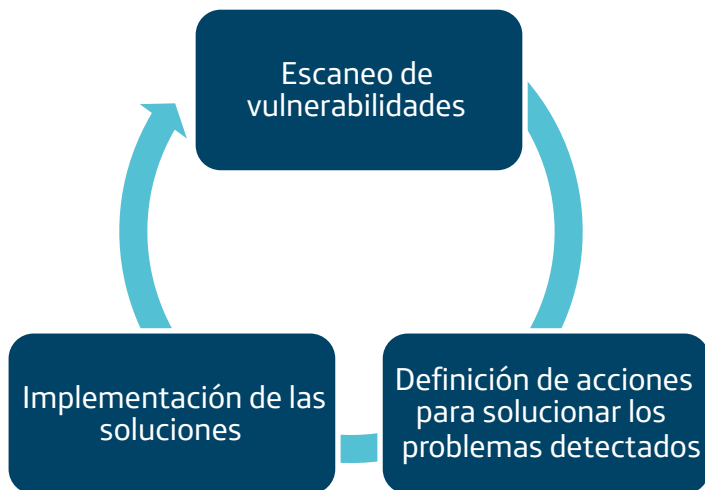
17. «A vision for cyber security detection analytics», Hewlett Packard, Business white paper.

18. «Proactive detection of network security incidents», Enisa.

19. «Cyber Security Monitoring and Logging Guide», CREST.

A la hora de establecer un programa de gestión de vulnerabilidades hay que tener en cuenta en primer lugar el tamaño de la empresa para abordarlo de acuerdo con sus posibilidades. Pero hay dos aspectos que es necesario establecer; en primer lugar, definir las responsabilidades de las personas que se encargarán de gestionarlo; en segundo, actuar de acuerdo con tres pasos básicos (ver la figura 3.3).

Figura 3.3 Pasos para afrontar la gestión de vulnerabilidades

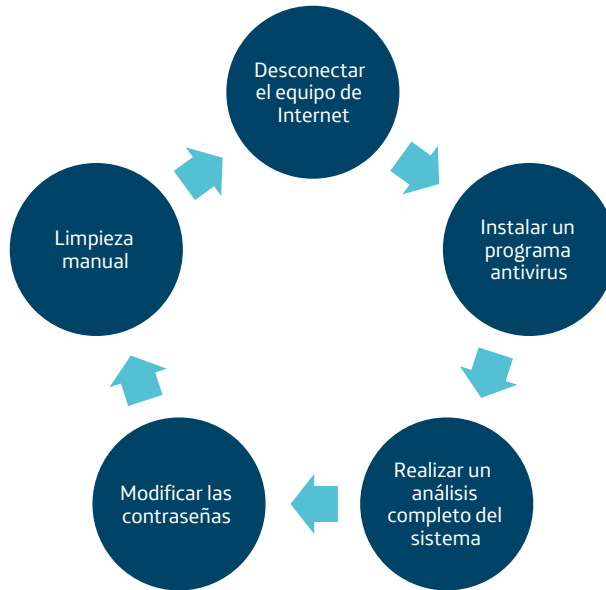


Fuente: Elaboración propia a partir de datos de ENISA.

3.3 Respuesta

Si desafortunadamente se ha producido un ataque y los equipos o sistemas se han visto infectados, es importante actuar en varios campos. Por un lado, dar una respuesta técnica y, si finalmente se ha producido un robo de identidad o robo de datos, acudir a las fuerzas y cuerpos de seguridad del Estado e iniciar acciones legales para que los delitos que se hayan podido cometer no queden impunes.

Para dar una respuesta técnica es primordial seguir cinco pasos con los que se podrá prevenir un robo de datos o acotar el impacto negativo del ataque.

Figura 3.4 Pasos a seguir ante un ciberataque

Fuente: Elaboración propia a partir de datos de CREST.

En primer lugar, hay que desconectar el equipo de Internet. Con la desconexión se podrá impedir que el virus que infectó el equipo continúe propagándose por la red y que se produzca una nueva infección después de la limpieza.

En segundo lugar, y si esto no se había realizado ya con anterioridad, instalar un programa antivirus. Como se ha comentado en el apartado anterior, es muy recomendable la utilización de herramientas proactivas mejor que reactivas, por lo que es deseable instalar un *software* que incluya capacidades de detección proactiva de amenazas. Si ya contábamos con un antivirus, otra acción fundamental es la de descargar y actualizar la base de firmas del antivirus para conseguir un análisis más eficiente del equipo.

En tercer lugar se debe realizar un análisis completo del sistema. Es muy importante analizar por completo todos los discos del equipo en busca de amenazas o daños.

La cuarta acción que se debe abordar es modificar todas las contraseñas de cualquier servicio que requiera autenticación. Con este procedimiento eliminaremos toda posibilidad de robo de credenciales por parte de los cibercriminales que se encuentran detrás del *malware*.

Por último, y en caso de resultar necesario, se debería realizar una limpieza manual porque no siempre es suficiente con escanear el sistema y realizar una limpieza automatizada. Para

poder llevar a cabo de una forma eficaz esta tarea, es recomendable identificar el tipo de *malware* responsable del ataque para buscar el método más adecuado de desinfección.

En cuanto a las acciones legales que se pueden emprender si se ha sufrido un ataque informático, un robo de datos o suplantación de identidad en Internet, la primera y más importante es la de denunciar el ataque ante los cuerpos y fuerzas de la seguridad del Estado o la OSI (Oficina de Seguridad del Internauta). Denunciar es esencial, ya que gracias a la denuncia es posible investigar y perseguir este tipo de delitos²⁰. Según el Ministerio del Interior, en 2014, el 95 % de los cibercrimitos quedaron impunes²¹; de ahí la importancia de denunciar.

Por otro lado, el legislador español poco a poco ha introducido actualizaciones y modificaciones con las que afrontar el fenómeno de la ciberdelincuencia. Uno de los primeros pasos fue la suscripción por parte de España del Convenio de Budapest, con el que se trató de dar una respuesta legal y uniforme al problema a través del Derecho Penal. Pero como esta forma de delincuencia ha seguido evolucionando y siguen apareciendo nuevos delitos, nuevamente nuestro país se ha visto en la necesidad de actualizar el Código Penal en esta materia. Con la Ley Orgánica 1/2015 se regulan nuevos tipos penales en este ámbito como son el delito de acoso electrónico (artículo 172 CP), delitos de descubrimiento y revelación de secretos (artículo 197), delitos de daños y delitos de interferencia ilegal en sistemas de información o datos (artículo 264), delitos contra la propiedad intelectual (artículo 270) y el de abusos con fines sexuales cometidos a través de Internet u otros medios de telecomunicación a menores (artículo 183 CP). Se quiere establecer una mayor protección ante ataques informáticos que supongan revelación de secretos o interferencias en los sistemas para robar información o datos adaptando los tipos penales a la nueva realidad²². El problema que aparece en el ámbito penal y legislativo es que el mundo digital y la ciberdelincuencia suelen evolucionar a mayor velocidad que el derecho con el que se pretende perseguir a los delincuentes y garantizar los derechos y libertades de los ciudadanos. La respuesta ante los ataques, tanto técnica como jurídica, debe intentar ser lo más ágil posible.

Veamos en más detalle estos dos elementos críticos en la respuesta ante ciberataques: los sistemas de recuperación que existen y la recolección de evidencias digitales que permitan emprender acciones legales contra los atacantes.

3.3.1 Sistemas de recuperación

Los sistemas de recuperación son una función que permite al usuario devolver el estado de su equipo y las aplicaciones al punto de partida anterior a que se haya producido un problema y así solucionarlo.

20. María Concepción Rayón Ballesteros y José Antonio Gómez Hernández, «Cibercrimen: Particularidades en su investigación y enjuiciamiento», *Anuario Jurídico y Económico Escorialense*, XLVII (2014), 209234/ISSN: 133-3677.

21. II Informe sobre cibercriminalidad 2014, Ministerio del Interior.

22. *Ibidem*.

Uno de los sistemas operativos pioneros en incluir esta función fue Microsoft en sus sistemas operativos de Windows. En la primera versión que se incluyó fue en Windows ME y, a partir de entonces, se ha introducido en todas las versiones del sistema operativo que le han seguido²³. En las primeras versiones, este sistema se basaba en un filtro de archivos que observaba los cambios que sufrían las diferentes extensiones, copiando los archivos antes de ser sobrescritos. Posteriormente, en las versiones a partir de Windows Vista, utiliza un Shadow System de restaurado que permite cambios de bloque en archivos ubicados en cualquier directorio de forma que reciben apoyo y son monitorizados con independencia de su ubicación. También permite realizar recuperaciones si la versión de Windows instalada no consigue limpiar el sistema.

Otro sistema operativo que ha introducido esta función ha sido Android. El *recovery* se basa en una partición con propiedades de arranque. Se ejecuta separado y paralelo al sistema operativo principal de Android. Las particiones en que se dividen son *boot/kernel* y *root/system*. Estas particiones se encuentran separadas del sistema de recuperación que contiene su propio kernel de Linux.

Como el dispositivo tiene su propio kernel, puede arrancar en el modo de recuperación incluso cuando el sistema se encuentra dañado. De esta forma, el *recovery* es su propio dueño y se complementa de forma independiente al resto de Android.

Gracias a que tiene su propio kernel, el dispositivo puede *bootear* en modo *recovery* incluso cuando el sistema está dañado de alguna forma. Mientras la partición de *recovery* se mantenga intacta, el usuario tiene una herramienta a mano para recuperar su *gadget* Android. Con este sistema, Android pretendía la realización de tres acciones. En primer lugar, solicitar actualizaciones de *software* al dispositivo *over the air*, también conocido por sus siglas OTA. Este ha sido el método oficial de actualización del *hardware*. En segundo lugar, poder borrar datos de usuario y el caché para dejar el dispositivo como si este viniese de fábrica. Por último, poder ejecutar herramientas externas desde la memoria SD²⁴.

En Apple, OS X Recovery incluye un conjunto de servicios para recuperar un equipo. OS X Recovery permite restaurar un equipo Mac desde una copia de seguridad, verificar y reparar los dispositivos conectados que utilizan la Disk Utility, comprobar la conexión a Internet u obtener ayuda online mediante Safari y, por último, instalar o reinstalar OS X²⁵.

Para que estos sistemas sean de verdadera utilidad para una organización, es fundamental realizar copias de seguridad con suficiente regularidad.

23. <http://windows.microsoft.com/en-us/windows7/restore-system-files-and-settings>

24. <http://hipertextual.com/archivo/2014/01/modo-recovery-android/>

25. <https://support.apple.com/en-us/HT201314>

3.3.2 Evidencias digitales / cumplimiento con la regulación

Por evidencia digital entendemos cualquier documento, fichero, registro o dato contenido en un soporte informático, susceptible de tratamiento digital y que puede ser utilizado como prueba en un proceso legal.

Las evidencias digitales resultan de gran utilidad para la seguridad en Internet, especialmente a la hora de perseguir posibles delitos que se hayan podido cometer. Las actividades en el entorno digital, y muchas de las acciones en el mundo físico, dejan un rastro digital. Estas evidencias pueden ayudar a establecer si un crimen se ha ejecutado o pueden proporcionar un enlace entre un crimen y su víctima o un crimen y su autor.

A la hora de probar un hecho ante la justicia, ya sea dentro del ámbito civil o del ámbito penal, la Constitución española reconoce en su artículo 24.2 el derecho a utilizar los medios de prueba pertinentes para nuestra defensa. En el mundo digital se generan nuevas fuentes de prueba que se sustentan en nuevos soportes, que a menudo desafían los conceptos del Derecho tradicional.

A la hora de concretar este mandato constitucional en el derecho de las nuevas tecnologías, es necesario buscar la definición de medios probatorios y la concreción de la validez de las evidencias digitales dentro de la normativa sustantiva y procesal. En el artículo 299 de la Ley de Enjuiciamiento Civil se enumeran de forma abierta y genérica los medios de prueba admitidos diciendo que serán pruebas válidas «los medios de reproducción de la palabra, el sonido y la imagen, así como los instrumentos que permiten archivar y conocer o reproducir palabras, datos, cifras y operaciones matemáticas llevadas a cabo con fines contables o de otra clase, relevantes para el proceso».

En el marco legislativo español, la admisibilidad de la prueba electrónica en los tribunales se encuentra regulada mediante disposiciones generales procedentes y aplicables a los medios de prueba tradicionales. Esto genera cierta inseguridad jurídica, ya que, en muchas ocasiones, los jueces son reticentes a aceptar este nuevo tipo de pruebas que surgen del desarrollo de las nuevas tecnologías.

De todas maneras, para que una evidencia digital sea válida debe cumplir con tres requisitos²⁶:

- Ser auténtica: debe poder probarse que la evidencia es veraz, que no ha sido modificada.
- Ser precisa: debe poder demostrarse su relación con el hecho de forma inequívoca.
- Ser suficiente: debe contener información suficiente para poder demostrar un hecho por sí misma, sin necesidad de otros elementos externos.

26. Gustavo Pineda Montano, «La evidencia digital», 27 de mayo de 2014.

Por ello es muy importante guardar registros electrónicos, ser capaces de identificar dónde se encuentran y garantizar la integridad de cualquier posible evidencia digital, que pueda permitir esclarecer cualquier vulneración de la seguridad de equipos o sistemas. Esto es especialmente relevante cuando se trabaja con servicios *cloud computing* o en la nube que, como veremos más adelante, pueden acarrear dificultades para controlar nuestra información y son menos transparentes, lo que puede afectar a la integridad de las evidencias y dificultar la comprobación de su autenticidad.

3.4 La inteligencia para dotar de eficiencia a las medidas de ciberseguridad

El carácter dinámico y cambiante de las amenazas cibernéticas obliga a la constante actualización y revisión de los sistemas de seguridad, lo que se traduce en que la ciberseguridad es un proceso costoso, en recursos económicos y en tiempo. Las amenazas afectan a todos, los Estados, las empresas y organizaciones y los ciudadanos. Por ello, compartir información y analizarla de forma eficiente puede ayudar a mejorar el nivel de seguridad y abaratar costes, ya que los esfuerzos se diversifican entre diferentes agentes. Esto requiere de una mayor colaboración entre tres tipos de agentes principales:

- Los cuerpos y fuerzas de seguridad de los Estados.
- Las entidades y empresas del mundo de la ciberseguridad.
- Las empresas y organizaciones de la sociedad civil²⁷.

La colaboración entre agentes mejora el conocimiento, mejora la información y permite dotar de mayor inteligencia a los sistemas de ciberseguridad. Todo ello requiere diversificar y ampliar las fuentes de información sobre las amenazas y analizarlas de forma conjunta, es decir, es necesario compartir información y que esta información sea compatible para poder ser analizada.

3.4.1 Análisis de información proveniente de fuentes diversas y búsqueda de correlación

El análisis de datos y la posibilidad de procesarlos rápidamente mejoran notablemente la capacidad de investigación y reducen el tiempo que se necesita para el descubrimiento de nuevas amenazas. Se trata de poder realizar análisis en tiempo real que permitan una efectiva toma de decisiones basadas en los riesgos.

El desarrollo de sistemas inteligentes, basados en el análisis de información y la búsqueda de correlaciones, es la respuesta a la necesidad de desarrollar políticas proactivas que busquen entender una amenaza antes de que un atacante pueda causar daño. Gracias al acceso

27. Doug Frankli, «Threat Intelligence Collaboration Leads to More Efficient, Comprehensive Cybersecurity», 7 de mayo de 2015.

a una gran cantidad de datos consolidados, es posible distinguir potenciales amenazas y priorizarlas, ya que son capaces de correlacionar estos datos con otro tipo de información, como por ejemplo las vulnerabilidades del sistema. Esto, como ya se ha mencionado anteriormente, requiere de una monitorización constante del comportamiento de la red para que la actividad inusual pueda distinguirse del comportamiento normal.

3.4.2 Fuentes de datos abiertas (OSINT–Open Source Intelligence)

Las fuentes de información OSINT son fuentes de información de acceso libre, gratuitas y desclasificadas. Por ello todo el conocimiento accesible a través de estas fuentes de acceso público se conoce como Open Source Intelligence (OSINT).

Son fuentes de datos abiertas las webs públicas, los blogs y las redes sociales, las bases de datos gubernamentales abiertas, los medios de comunicación, las bibliotecas online, etc., es decir, toda la información libremente accesible y gratuita de Internet.

Las fuentes de información abiertas son esenciales para generar un sistema de ciberseguridad eficiente porque permiten conocer el entorno y mejorar la capacidad de predicción e identificación de amenazas a través de un análisis prospectivo. Por ejemplo, una serie de comentarios en una red social pueden ayudarnos a prevenir un ataque. Por tanto, OSINT puede ayudarnos a desarrollar un sistema más proactivo.

La utilización de fuentes de datos abiertas y la generación de un proceso OSINT requiere de los siguientes pasos:

Figura 3.5 El ciclo del OSINT



Fuente: Incibe.

En primer lugar está la *fase de requisitos*. En esta fase se establecen todos los requerimientos que se deben cumplir a la hora de satisfacer o resolver el problema que ha originado el desarrollo del sistema OSINT.

Después debemos *identificar las fuentes de información relevantes*. Esto consiste en especificar a partir de qué requisitos, que hemos establecido en la primera fase, vamos a seleccionar las fuentes de interés en las que recopilaremos la información. Resulta muy importante la identificación de las fuentes relevantes, porque el volumen de información disponible en Internet es ingente; por lo que, si identificamos y concretamos las fuentes, conseguiremos optimizar el proceso de adquisición de información.

En tercer lugar está la *etapa de adquisición*. Aquí es donde se obtendría la información a partir de los criterios que hemos establecido tanto en la fase de requisitos como en la identificación de fuentes relevantes.

Una vez adquirida la información se *procesa* para darle un formato que nos permita su análisis posterior.

La *fase de análisis* es aquella donde se genera inteligencia a partir de los datos que hemos recopilado y procesado. Esto nos permitirá relacionar la información de distintos orígenes, en busca de patrones con los que llegar a alguna conclusión significativa²⁸.

Por último está la *presentación de inteligencia*. Aquí se presenta la información obtenida de una forma que resulte eficaz, útil y comprensible para una correcta explotación que permita tomar decisiones.

3.4.3 Profiling de usuarios–Atribución

El *profiling* de usuarios consiste en la creación y gestión de perfiles. Un perfil de usuario posee información sobre el usuario y permite al sistema incrementar la calidad de sus adaptaciones. Además, a los perfiles es a los que se les asignarán los roles con los que dicho perfil podrá actuar en las tareas computacionales que desarrolla en la organización o en la empresa.

El *profiling* de usuarios, y su gestión, resulta importante respecto a la seguridad de los equipos y redes desde el punto de vista de la información aportada en relación con su actividad, que convenientemente tratada y analizada proporciona inteligencia para mejorar la ciberseguridad.

Para incrementar la inteligencia que brinda la información relacionada con los perfiles de usuario, resulta adecuado dividirla en tres categorías: datos del usuario, datos de utilización y datos del ambiente.

28. https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/osint_la_informacion_es_poder

Figura 3.6 Categorías del *profiling* de usuarios

Fuente: Elaboración propia a partir de datos de la Universidad de Salamanca.

Los datos del usuario constituyen la información que se utiliza para establecer las características de este. Las principales características que modelan y utilizan los sistemas son las demográficas, el conocimiento del usuario sobre el tema, los objetivos y plan del usuario, sus preferencias, sus intereses y los rasgos individuales de personalidad. En cuanto a los datos de utilización, es la información que va a comprender la interacción del usuario con el sistema. Estos datos podrán ser observados de una forma directa o se adquirirán mediante un análisis de los datos observables. Por último, los datos del ambiente se encuentran conformados por el entorno del usuario y no están directamente relacionados con el mismo. Aquí podremos estudiar cuestiones como la frecuencia de utilización, la correlación entre situación y acción y secuencias de acciones.

Pero la obtención de estos datos que hemos comentado no siempre resulta fácil. En numerosas ocasiones necesita de un procesado para adquirir el contenido inicial de los perfiles. El método más común para conseguir información es dejar que el propio usuario provea los datos que se requieren de forma explícita. También se pueden utilizar reglas de adquisición como método con el que generar suposiciones acerca del usuario. Una tercera forma es la de reconocer el plan de usuario. Este método razona sobre los objetivos que este persigue y la secuencia de acciones que puede realizar para lograrlos. Por último, también se puede obtener la información partiendo de otros. Este método es una forma muy simple de adquisición. Los estereotipos asumen un principio por el que si un usuario se encuentra en una categoría determinada, entonces tendrá características y comportamientos similares a los miembros de esa categoría en un conjunto de circunstancias²⁹. Por eso, resulta fundamental proteger este proceso de emisión de datos para la creación de un perfil y el almacenamiento de estos. Con perfiles seguros nos aseguraremos de que la persona que puede realizar determinadas tareas de la organización es la realmente autorizada y no alguien externo a esta con otra serie de intereses.

3.4.4 Compartición de datos de incidentes entre corporaciones

Actualmente las empresas han asumido que tienen que ser digitales o que tienen que ir digitalizándose. Uno de los problemas fundamentales es la segmentación de información dispo-

29. Rui Alexandre Pereira Pinheiro da Cruz, Francisco José García Peñalvo y Luis Alonso Romero, «Perfiles de usuarios para la adaptatividad de interfaces web», Universidad de Salamanca.

nible por las empresas, ya que muchas veces ciertas anomalías que vistas de una forma individual no se pueden considerar ataques, si se producen de forma simultánea en muchas empresas del sector, sí se pueden identificar como un ataque. Para luchar contra ello, la compartición de datos entre corporaciones resulta fundamental y facilita que se pueda dar una respuesta más rápida y contundente a las amenazas.

En este sentido, y como ejemplo de iniciativas que parten tanto del ámbito privado como del público, han surgido alianzas entre empresas, como la de Telefónica con la Cyber Threat Alliance³⁰, o se han aprobado leyes (a veces algo polémicas) como la Ley de Compartición de Información de Ciberseguridad en Estados Unidos.

Telefónica, al desarrollar su alianza con otras grandes corporaciones dentro de la Cyber Threat Alliance, pretende situarse a la vanguardia a la hora de prevenir ciberataques como los que experimentaron Adobe o eBay, cuando dejaron expuestos casi 300 millones de registros de usuarios³¹. A través de la Cyber Threat Alliance, Telefónica y el resto de las organizaciones que la conforman pueden disponer de un grupo de profesionales de la ciberseguridad elegidos por todos los miembros. Estos profesionales han sido seleccionados por su experiencia en la resolución de estos problemas para otras compañías. Así, lo que se pretende es que, a través de la alianza, las empresas que la conforman puedan compartir el conocimiento que ya han adquirido y su experiencia para que el resto de las compañías puedan adelantarse o saber cómo actuar ante amenazas similares a las que ellos ya han sufrido. También se pretende poder desarrollar nueva tecnología y nuevas herramientas con las que protegerse y ampliar su catálogo de servicios de ciberseguridad³².

En cuanto a la Ley de Compartición de Datos, el Gobierno de Estados Unidos pretende luchar contra los ciberataques que se producen en el ciberespacio compartiendo datos entre empresas privadas y el Gobierno federal. Las empresas compartirán voluntariamente con el Gobierno federal aquellos datos que crean que pueden constituir una ciberamenaza.

El proyecto de ley crea un sistema federal de agencias para recibir la información sobre amenazas de las compañías privadas. Pero este sistema no otorga inmunidad legal a las compañías que se acojan a él en materia de cumplimiento de las obligaciones que estas tienen para proteger la privacidad de los datos de sus usuarios. Es más, se incluye una provisión por la que no se podrán utilizar aquellos datos personales que resultan irrelevantes para la ciberseguridad. Por tanto, las agencias gubernamentales creadas mediante esta ley solo podrán utilizar aquellos datos compartidos por las empresas que resulten de utilidad para protegerse de una ciberamenaza. También se podrán usar estos datos compartidos, y que cumplan la

30. <http://cyberthreatalliance.org>

31. <http://blogthinkbig.com/telefonica-une-fuerzas-con-la-cyber-threat-alliance>

32. *Ibidem*.

premisa de relevancia, como evidencia de delitos relacionados con la fuerza física y no solo con los delitos relacionados con las ciberamenazas.

Los críticos de esta ley advierten del peligro que esta puede suponer para la privacidad de los internautas a pesar de que la misma prohíba que se utilicen datos que no son relevantes para la ciberseguridad. Porque, según se desprende del texto, no se evita que se faciliten a las agencias gubernamentales. Lo que se evita es que estos datos sean utilizados por ellas.

3.4.5 Diversidad de estándares

Como se ha comentado en los apartados anteriores, resulta necesario mantenerse actualizado en relación con la creciente complejidad de los ataques, y es fundamental focalizar los esfuerzos en la detección, prevención y respuesta en las primeras fases del ciberataque. También se ha presentado la compartición de datos entre las empresas que han experimentado incidentes de seguridad como una de las principales armas que contribuye al mejor conocimiento de la evolución de los ataques. El problema surge cuando la información sobre estos ataques se encuentra almacenada en soportes o formatos que no son compatibles con los que utiliza otra empresa u otro proveedor de ciberseguridad. Por eso se hace necesario crear un campo común donde estandarizar la información sobre amenazas. Tal y como se ha analizado a lo largo del documento, resulta más eficaz la prevención que la reacción y cuanto más fácil sea compartir el conocimiento sobre los ciberataques, mejor se podrán prevenir.

Entre las especificaciones y técnicas definidas para la compartición de información sobre incidentes de seguridad destacan los siguientes:

- *Trusted Automated Exchange of Indicator Information (TAXII)*
- *Cyber Observable eXpression (CybOX)*
- *Structured Threat Information eXpression (STIX)*

Estas especificaciones juegan un papel importante en el proceso de estandarización de compartición de información de incidentes de seguridad. Son varias iniciativas para impulsar una comunidad abierta de datos y un conjunto de especificaciones gratuitas, que habilitan una mejor gestión de la ciberseguridad mediante el intercambio automatizado de información sobre ciberamenazas.

TAXII abarca un conjunto de especificaciones para el intercambio de información sobre ciberamenazas con las que se pretende ayudar a las organizaciones cuando comparten información con sus socios³³. TAXII posee tres modelos diferentes para compartir información. El

33. <https://stixproject.github.io/oasis-faq.pdf>

primero es el denominado HUB and Spoke, que consiste en un centro de distribución. Otro es el Source/Subscriber, en el que una organización es la única fuente de información. Y en tercer lugar está el modelo Peer to Peer, que permite que varias organizaciones compartan su información entre ellas.

Los servicios contemplados por TAXII para compartir la información son cuatro: la de bandeja de entrada, encuestas, gestión de recogida de información y el de descubrimiento. El primer servicio consiste en poder recibir directamente el contenido. El segundo nos permite requerir contenido. El tercero, conocer y suscribirse a las colecciones de datos y, por último, el cuarto servicio es el que permite aprender qué servicios admite un sistema y cómo interactuar con ellos.

En cuanto a CybOX, proporciona una estructura común para la especificación, captura, caracterización y comunicación de eventos que son observables en las operaciones de red y de los sistemas. Estos eventos pueden ser dinámicos o propiedades de mejora. Es decir, puede ser tanto un mensaje de correo electrónico que es recibido desde una específica dirección como una conexión de red que se establece hacia una dirección concreta o la modificación de una clave de registro.

En último lugar, STIX se refiere a un lenguaje estandarizado para representar la información de las ciberamenazas.

Podemos concluir que tanto TAXII, STIX o CybOX como el resto de las iniciativas se presentan como un marco impulsado por la comunidad informática con el que se quiere hacer frente a las necesidades emergentes de compartir información sobre amenazas que incluya automatización, seguridad, consistencia, riqueza de expresión y, lo más importante, interoperabilidad. Por eso pretende ser un conjunto de directrices con las que fomentar un mayor intercambio de información sobre la amenaza, al incorporar protocolos y mecanismos existentes en su uso por diferentes comunidades, con la intención final de apoyar en su uso todo el conjunto de información sobre amenazas cibernéticas del que se dispone.

Nuevos escenarios y desafíos de la ciberseguridad

4.1	BYOD (<i>Bring Your Own Device</i>)	44
4.2	<i>Cloud computing</i> y <i>big data</i>	47
4.3	Internet de las cosas (<i>Internet of Things</i>)	51
4.4	Internet industrial	54
4.5	Apps móviles	58
4.6	Múltiples identidades digitales: el reto para protegerlas e identificarlas con la identidad física	61
4.7	Desafíos legales de la ciberseguridad	65

Como se ha comentado en la introducción, nos hallamos ante una situación en la que los usuarios y las empresas somos conscientes de la importancia vital que tiene la seguridad en nuestras vidas, una vez que lo digital se encuentra en todos los ámbitos y actividades. Por una parte se observa que todavía no se han interiorizado los cambios que se han producido en los últimos años; por otra, nuevas tendencias tecnológicas como BYOD, IoT, *cloud computing*... suponen nuevos desafíos relativos a la seguridad. El dar una respuesta adecuada a dichos desafíos será clave para conseguir que los servicios y aplicaciones de la sociedad de la información se desarrollen y sean utilizados masivamente por la población.

4.1 BYOD (*Bring Your Own Device*)

En la actualidad, nos encontramos en un entorno en el que se están diluyendo las barreras entre el ámbito personal y el ámbito profesional de los empleados, como muestran numerosos análisis; por ejemplo, un estudio sobre trabajadores de oficina según el cual el 75 % realiza tareas personales en el tiempo de trabajo y el 77 % realiza tareas relacionadas con su trabajo en su tiempo personal³⁴. Un fenómeno asociado a esta situación y a la proliferación de dispositivos de movilidad dentro de la empresa, principalmente el *smartphone*, es que cada día es más frecuente que se utilicen los mismos recursos para realizar la actividad de la empresa y para las tareas de índole personal. De hecho, la empresa Gartner, Inc. afirma que «el BYOD es el cambio más radical en la computación de cliente desde la introducción de los PC en los lugares de trabajo». Este fenómeno que ya afectaba a 350 millones de empleados en el año 2014 en el mundo, se cree que continuará creciendo durante los próximos años dado que las empresas que han introducido estas políticas han reportado incrementos en la eficiencia y en la productividad (Bradley et al, 2013). También se observa que cada vez son más los empleados que utilizan sus dispositivos personales en los entornos de trabajo, independientemente de las medidas que las empresas tomen anti-BYOD (Fortinet, 2012).

Asociado a esta tendencia de que los usuarios empleen dispositivos durante su actividad laboral, es habitual que utilicen también sus propias aplicaciones en lo que se ha venido a denominar BYOA (*Bring Your Own Application*). Así, el 70 % de las empresas (81 % en el caso de pequeñas y medianas empresas) se encuentran en la situación en la que los empleados utilizan apps de carácter personal en dispositivos utilizados en el trabajo, incluso se llega a cuantificar esa situación en 21 apps de media en cada organización. Se trata además de una tendencia que los expertos consideran que seguirá creciendo, opinión que es mostrada por el 42 % de ellos. Mientras, el 35 % cree que su utilización se mantendrá, el 11 % que disminuirá debido a la prohibición de las empresas y el 10 % que disminuirá debido a que las empresas ofrecerán todas las apps necesarias. Llama la atención que en muchas ocasiones (64 %) existen aplicaciones corporativas que ofrecen esas funcionalidades, en lo que se ha llamado «efecto Dropbox».

34. Samsung. Ámbito Europa. Bases: Trabajadores de oficina.

Prácticamente todas las empresas, tanto las que han mostrado una actitud favorable a permitir BYOD como aquellas que se han posicionado en contra, son conscientes de que es una tendencia que de una u otra forma les afecta, por lo que se han realizado diversos estudios en los que se analiza el impacto en las organizaciones de la utilización de los dispositivos personales en los entornos laborales. Entre los efectos positivos que se han encontrado destacan:

- *Accesibilidad*: la utilización de los dispositivos personales facilita el acceso a los recursos de la empresa, lo que supone la posibilidad de trabajar desde cualquier lugar y en cualquier momento.
- *Conveniencia y flexibilidad*: BYOD aumenta la flexibilidad de los empleados a la hora de trabajar, al facilitar el trabajo en remoto, sobre todo en los trabajos en los que no se necesita el acceso a un entorno especial, sino a cierta información online.
- *Satisfacción del empleado*: la mayoría de los empleados se encuentran más satisfechos con la utilización de sus propios dispositivos y además agradecen la comodidad de no tener que llevar diversos dispositivos. También suelen estar más acostumbrados a utilizar sus propios dispositivos, lo que supone una reducción de los tiempos de aprendizaje.
- *Incremento de la productividad y de la innovación*: dado que la mayoría de los usuarios están más satisfechos utilizando sus propios dispositivos, también suelen ser más productivos. Además, en este caso tienden a actualizar continuamente las aplicaciones, lo que puede suponer un efecto positivo en la innovación de la empresa.
- *Reducción de costes*: la utilización de los dispositivos personales en los entornos de trabajo puede suponer una reducción de costes para la empresa e incluso para el trabajador.

4.1.1 Necesidades de seguridad

Dados estos beneficios, el BYOD empieza a ser en muchas empresas la norma en lugar de la excepción. Esto supone una serie de problemas que la empresa debe ser capaz de encarar. En primer lugar, la empresa debe crear y gestionar nuevos procesos que tengan en cuenta esta nueva situación. En segundo lugar, la seguridad debe estar presente a lo largo de todo el proceso, para evitar fugas de datos, de privacidad y ciberataques. Cuando un dispositivo móvil accede a la red y de esta manera a los recursos de la empresa, es más difícil evitar que ciertas trazas de información personal caigan en el poder de terceras entidades. Además, los dispositivos afectados por BYOD suelen ser dispositivos pequeños, fáciles de perder, que dejan al alcance de quien los encuentre información que puede tener un gran valor.

El acceso sin un control adecuado y sin restricciones a los sistemas de la empresa puede suponer una puerta para la entrada de *malware*. Adicionalmente un acceso sin restriccio-

nes puede significar un consumo de los recursos y del ancho de banda excesivo que repercute en el rendimiento de los sistemas. Por ejemplo, si no hay control de accesos para los dispositivos móviles, estos se conectarán continuamente al SSID (*Service Set Identification*), lo que supone una mayor utilización *hardware* de recursos. De esta forma, muchos dispositivos entrando continuamente en la misma red pueden reducir su capacidad e incluso provocar su caída.

Otro de los problemas que se reporta más comúnmente en el BYOD es la convivencia de gran cantidad de sistemas operativos y de diferentes versiones, diversidad que es difícil de gestionar y que puede suponer en muchas ocasiones agujeros de seguridad. Además, en las empresas que tienen un número muy alto de dispositivos tanto de carácter empresarial como personales, puede llegar a ser muy difícil de mapear cuáles son los recursos a los que debe tener acceso cada dispositivo. Todo esto puede suponer que se permita el acceso a recursos que no se debería a un empleado o incluso a otras personas que no pertenezcan a la organización.

4.1.2 Soluciones de seguridad

Como se observa, los problemas de seguridad que puede generar el BYOD son muy diversos, y dado que es una tendencia difícil de evitar y que incluso emerge espontáneamente en las empresas, es necesario al menos tomar dos acciones. Una, concienciar a los empleados de los riesgos y de la necesidad de que adopten medidas mínimas de seguridad activa, como por ejemplo no entrar en páginas de dudosa reputación o evitar prestar sus dispositivos a terceros. Por otra parte, la empresa debe implementar una estrategia respecto a BYOD. Esta estrategia puede estar basada en diferentes enfoques, como se muestra a continuación.

- *Enfoque orientado a la red*: este enfoque, cuya idea fundamental es el control de acceso a la red, conocido como NAC (*Network Access Control*), supone que la red controla qué dispositivos acceden al sistema. Algunas soluciones con este enfoque son las soluciones BYOD de Cisco y Meru Networks. Tiene algunas ventajas, como que segmenta la red y facilita la encriptación y la autenticación, y además permite crear redes virtuales de área local que mantengan los dispositivos en diferentes segmentos. No obstante, también se encuentran desventajas como la compatibilidad con los diferentes tipos de dispositivos, la saturación de la red en el caso de acceso múltiple a contenidos pesados o que se permita el acceso a dispositivos modificados para introducir *malware*.
- *Enfoque orientado a la gestión de dispositivos móviles*: el enfoque orientado a la gestión de dispositivos móviles, conocido como MDM (*Mobile Devices Management*) se basa en una plataforma *software* que monitoriza y gestiona todos los dispositivos móviles. Su funcionalidad incluye la distribución centralizada de aplicaciones, datos y ajustes.

tes de configuración para todos los dispositivos que se encuentren en la red. Estas plataformas pueden utilizar herramientas estándares como Microsoft Exchange ActiveSync, Google Device Manager o Apple Profile Manager. La ventaja que tiene este modelo es que provee un enfoque unificado para gestionar todos los dispositivos móviles. En cambio, en ocasiones, puede ser un poco confuso, sobre todo cuando hay una gran diversidad de dispositivos y sistemas operativos.

- **Virtualización.** La virtualización permite a las aplicaciones funcionar en servidores *back-end* en vez de en los dispositivos móviles, con lo que tanto las aplicaciones como los datos de empresa no se encontrarían en los propios móviles. De este modo es más sencillo separar el ámbito privado del ámbito personal. Tiene la ventaja de que esta forma de trabajo permite evitar las limitaciones de los dispositivos, ya que el procesamiento se lleva a cabo en servidores que no están sujetos a las mismas restricciones. Este enfoque también permite actualizar fácilmente las aplicaciones y evitar el contagio de virus y otro *malware*. Por el contrario, no siempre es fácil o es posible virtualizar las aplicaciones; la virtualización puede suponer que funcionen más lentas de lo habitual y, además, tiene la desventaja de que es necesario tener en todo momento acceso a Internet.
- **Enfoque centrado en el móvil.** Este enfoque supone mantener la seguridad en el propio dispositivo mediante un sistema MDM instalado por el fabricante. En general, el dispositivo móvil posee una doble SIM, una que se utiliza para el entorno personal y otra para el entorno profesional. Se refiere al enfoque preferido cuando hablamos de entornos en los que existen unos requisitos de seguridad elevados. La arquitectura del dispositivo se puede construir basada en capas de seguridad que permitan por ejemplo el encriptado de las llamadas y las comunicaciones o el encriptado de la información interna. Los dispositivos vendrían preconfigurados, tanto en lo relativo a aplicaciones como a ajustes que limiten funciones específicas dependiendo de la localización o de la red conectada. El mayor problema de este enfoque es que puede afectar a la experiencia del usuario y la necesidad de utilizar aplicaciones preinstaladas. Además puede haber problemas con el funcionamiento del *hardware* de cifrado en las microtarjetas del móvil. Estas tecnologías que a veces se engloban bajo el término *containerization* pueden dar lugar a vulnerabilidades que dejen escapar datos corporativos.

4.2 Cloud computing y big data

4.2.1 Necesidades de seguridad

Con la aparición del *cloud computing* se ha creado una amplia gama de posibilidades tanto para empresas y organizaciones (públicas o privadas) como para particulares, ya que ha hecho posible la existencia de sistemas que ofrecen recursos de procesamiento y almacenamiento de datos bajo demanda y la creación de bases de datos de alta escalabilidad.

Sin embargo, la seguridad se está presentando como una de las barreras que tiene que vencer este tipo nuevo de servicios para desarrollar todo su potencial. Existen cinco riesgos principales que centran actualmente el debate en torno a la seguridad y el *cloud computing*³⁵.

Uno de los riesgos más importantes a la hora de utilizar el *cloud computing* es la pérdida de control en el uso de las infraestructuras de la nube. Esto sucede porque el cliente cede necesariamente control al proveedor de la nube en algunos asuntos que pueden afectar a la seguridad. Además, los acuerdos de nivel de servicio (SLA, en sus siglas en inglés) pueden no ofrecer un compromiso concreto por parte del proveedor de la nube para prestar dichos servicios, con lo que deja espacio para potenciales problemas de seguridad.

Otro problema es el *Lock-In*, término que se refiere a la falta de herramientas, procedimientos y servicios de interfaz que puedan garantizar la seguridad de los datos y las aplicaciones cuando se lleva a cabo la portabilidad a otro proveedor. Por tanto, pueden aparecer problemas cuando una organización o una empresa han externalizado los servicios de almacenamiento, o de gestión de las infraestructuras de almacenamiento, y se quiere cambiar de un proveedor a otro, migrar los datos a otro sistema o volver a gestionarlos internamente. Este tipo de técnicas introduce una dependencia de los proveedores de servicios *cloud* para la provisión de estos servicios, sobre todo para la portabilidad de datos.

Los fallos de aislamiento también son otros de los riesgos que entraña el *cloud computing*. Esto se debe a que una de las características con la que operan estos sistemas es la tenencia múltiple (*multi-tenancy*) y la compartición de recursos. Estos fallos se producen, en ocasiones, a la hora de aislar y separar los mecanismos de almacenamiento, la memoria, el enrutado o diferentes usuarios que han contratado servicios de la nube. Sin embargo, es necesario precisar que los ataques a los mecanismos de aislamiento son mucho menores y mucho más complicados de penetrar por un atacante que con los sistemas operativos tradicionales.

En cuanto al cumplimiento de requisitos, podemos encontrar riesgos importantes a la hora de invertir en certificaciones externas de seguridad o calidad de los servicios, que presta la empresa u organización, cuando se están utilizando servicios en la nube. Estos problemas se dan porque, en muchas ocasiones, el proveedor de la nube no puede reportar evidencias de sus propios procesos de cumplimiento o porque tampoco se permite al usuario auditar a su proveedor sobre el cumplimiento de sus políticas internas de seguridad. Así, estos puntos pueden conllevar que una empresa no pueda cumplir con sus propios requisitos al no saber cuál es el trato que está recibiendo la información que ellos han almacenado en el servicio *cloud* que tienen contratado.

35. M. Mackay, T. Baker, A. Al-Yasiri, «Security-oriented cloud computing platform for critical infrastructures», Elsevier.

Otro riesgo más es el de la gestión de interfaces comprometidas. Con los servicios de la nube para almacenar datos, la gestión de las interfaces se realiza a través de Internet. Este medio, a pesar de ser más rápido y más económico para gestionar grandes cantidades de información, entraña ciertos riesgos al estar expuesto al tráfico de Internet. Especialmente cuando se combinan accesos remotos y navegadores web que son más vulnerables a los ataques.

A estos riesgos y problemas, a los que aún no se les ha encontrado una respuesta adecuada y efectiva, se les suma la dificultad de borrar datos de forma efectiva y segura y los riesgos propios de sufrir ataques por parte del propio personal que gestiona las infraestructuras del proveedor de servicios *cloud*. El primero se debe a que los sistemas *cloud* realizan migraciones de la información entre los diferentes recursos de la nube para su almacenamiento. Si estos datos no se borran efectivamente en todas las fases de la evolución, podrían caer en manos de personas no autorizadas. En cuanto al segundo problema, para gestionar los servidores de almacenamiento del proveedor de servicios *cloud* se tienen que crear perfiles con acceso a puntos donde un tercero (la compañía que utiliza los servicios *cloud*) tiene almacenada información que puede resultar muy sensible. Por este motivo, las políticas del proveedor de servicios *cloud* deben ser muy estrictas para controlar a su propio personal y el tratamiento que hacen con la información almacenada por terceros.

Por todo lo expuesto anteriormente, el *cloud computing*, a pesar de su enorme potencial, cuenta con una serie de debilidades ligadas a la seguridad en las que actualmente se está trabajando³⁶.

En lo que se refiere a las soluciones *big data*, este nuevo paradigma tecnológico puede suponer, desde el punto de vista de la seguridad, tanto una amenaza como una oportunidad. Como se ha visto anteriormente, el análisis de grandes cantidades de información es una gran oportunidad para mejorar la inteligencia de los sistemas de ciberseguridad y la prevención de incidentes de seguridad.

Sin embargo, el almacenamiento y tratamiento de enormes cantidades de datos supone un riesgo para la seguridad, ya que filtraciones o robos de información pueden tener importantes efectos legales y reputacionales para una organización.

El *cloud computing* y el *big data* van inexorablemente unidos, pues es poco probable que una organización almacene *in house* tal cantidad de datos. Por ello, los riesgos para la seguridad que ya hemos mencionado para el *cloud computing* son, en general, aplicables al *big data*.

Otros riesgos más concretos a los que se enfrenta el *big data* son³⁷:

36. Daniele Catteddu and Giles Hogben, «Cloud computing: Benefits, risks and recommendations for information security», ENISA.

37. Peter Wood, «How to tackle big data from a security point of view». <http://www.computerweekly.com/feature/How-to-tackle-big-data-from-a-security-point-of-view>

- Al tratarse de una tecnología nueva, el desconocimiento por parte de las organizaciones que lo aplican puede hacer que sea más vulnerable.
- La autenticación de usuarios y el acceso a los datos desde múltiples ubicaciones pueden no estar suficientemente controlados.
- Se puede ofrecer una oportunidad significativa para la entrada de datos maliciosos o para una inadecuada validación de los datos.

4.2.2 Soluciones de seguridad

Dentro de los sistemas tradicionales de seguridad, la encriptación de los datos de la red y la resiliencia de la red (que es la habilidad de proveer y mantener un nivel aceptable del servicio con el que poder hacer frente a los fallos y los retos que surgen diariamente por la utilización de la red) son las medidas de seguridad de mayor importancia³⁸.

El cifrado resulta fundamental para la protección de infraestructuras críticas que se van a servir de la nube³⁹. A través de los protocolos de capa 2 y 3 del modelo OSI se puede proveer de unos niveles aceptables de aseguramiento sobre la seguridad de conexión⁴⁰.

En cuanto a la resiliencia, tras asegurar la infraestructura de la nube y sus comunicaciones, se necesita conseguir que la conexión resulte confiable. Para ello se requerirá un nivel constante y permanente de conectividad con el que asegurarnos de que no se puede producir ninguna interrupción del servicio que le afecte con severidad. Hay dos aspectos fundamentales que tener en cuenta. Uno es la necesidad de reforzar el mecanismo de enrutado y otro prevenir los ataques malévolos al servidor. En el primer caso se necesita mejorar la arquitectura mediante un fortalecimiento del enrutado, que lo haga más fiable y ofrezca una garantía sobre la conexión de extremo a extremo. En el segundo, es necesario proteger la conectividad de ataques, como los de Denegación de Servicios Distribuidos (DDoS, según sus siglas en inglés), que han hecho populares organizaciones como Anonymus y que se han vuelto un quebradero de cabeza para los administradores IT⁴¹. Este tipo de ataques consiste en una saturación o sobrecarga de un servicio o recurso que finalmente provocará que un servidor deje de funcionar o responder o que funcione de forma intermitente o más lenta de lo que debería funcionar. Por tanto, un ataque DDoS se produce cuando una cantidad elevada de computadores se conectan al mismo servicio de forma simultánea y no es capaz de dar respuesta a cada una de las solicitudes y deja de ser accesible o de responder a usuarios legítimos que realmente están trabajando con el mencionado servidor. En este campo aún se siguen buscando

38. M. Mackay, T. Baker, A. Al-Yasiri, «Security-oriented cloud computing platform for critical infrastructures», Elsevier.

39. https://www.schneier.com/blog/archives/2012/11/encryption_in_c.html

40. M. Mackay, T. Baker, A. Al-Yasiri, «Security-oriented cloud computing platform for critical infrastructures», Elsevier.

41. <https://www.segu-info.com.ar/articulos/115-evitar-ataque-ddos-anonymous.htm>

fórmulas efectivas de protección porque hasta ahora las que se han puesto en marcha no se han mostrado infalibles o efectivas⁴².

En el ámbito del *big data*, el mecanismo más efectivo para hacer frente a los riesgos inherentes es el cifrado de los datos, que asegura la protección de los mismos desde el principio del proceso hasta el final y que solo sean utilizados por el personal autorizado a trabajar con ellos. También las soluciones de control de acceso granular están resultando muy útiles para que los administradores puedan acceder y compartir los datos de una forma más selectiva y precisa, al prevenir el mismo problema que con la encriptación. Como se ha comentado en repetidas ocasiones a lo largo del capítulo anterior, también es muy importante la monitorización continua para estar informados en todo momento de si se ha producido un ataque y así poder evitar de la forma más rápida posible una pérdida de información delicada⁴³.

4.3 Internet de las cosas (*Internet of Things*)

Internet de las cosas es una de las tendencias tecnológicas sobre las que más se ha debatido en los últimos años y que en la actualidad se considera que ha conseguido un nivel de madurez adecuado para provocar un impacto disruptivo en el desarrollo de la sociedad de la información y en el desarrollo de nuevos servicios y aplicaciones. Si bien los beneficios que se pueden obtener de conectar gran cantidad de objetos a Internet llevan varios años estudiándose, lo novedoso de estos últimos años es que ya se están realizando gran cantidad de pruebas en el ámbito del gran público o en otros entornos, como las ciudades inteligentes, y otros sectores con un gran peso económico, como el transporte, la salud... Las previsiones de crecimiento son espectaculares y si en la actualidad se calcula que existen 3.750 millones de objetos conectados a Internet, en el año 2020 esta cifra se multiplicará por más de seis hasta llegar a los 25.000 millones. La conexión de estos objetos, generalmente de pequeño tamaño, es posible debido al progreso de muchas tecnologías: miniaturización de componentes, menor consumo de energía, sensores casi microscópicos... No obstante, para que las previsiones de crecimiento se cumplan y se lleguen a desplegar estos objetos conectados de forma masiva en entornos diversos como las ciudades o los centros fabriles, será necesario continuar con esta evolución y que se entreguen módulos con capacidad de conectividad a muy bajo coste (entre 1 y 5 euros), cuya fuente de alimentación les permita operar durante años sin necesidad de ninguna intervención o, incluso, que sean capaces de captar energía del ambiente y puedan funcionar de forma autónoma desde el punto de vista energético.

Una de las consecuencias del despliegue masivo del Internet de las cosas es la posibilidad de una mayor interacción con el entorno en lo que se viene a denominar «ambientes inteligentes» o «*smart*». Ya se empieza a hablar de «*smart city*», «*smart home*», «*smart school*» o

42. M. Mackay, T. Baker, A. Al-Yasiri, «Security-oriented cloud computing platform for critical infrastructures», Elsevier.

43. Sreeranga Rajan, Fujitsu, «Top Ten Big Data Security and Privacy Challenges», Cloud Security Alliance.

«*smart vehicle*». Y es que el gran potencial de la conexión de todos estos objetos se encuentra en su capacidad de actuar de forma coordinada entre ellos, a lo que han contribuido otras tendencias tecnológicas como la computación en la nube, *big data* o inteligencia artificial. De esta forma ya no deben considerarse objetos conectados u objetos inteligentes de una forma aislada, sino de entornos enteros que son capaces de entender situaciones, y que se adaptan y reaccionan e incluso llegan a comunicarse con las personas.

4.3.1 Necesidades de seguridad

El Internet de las cosas supone que millones de dispositivos se encuentren continuamente generando datos y, lo que es más relevante desde el punto de vista de la seguridad, compartiendo esos datos en Internet. Una tendencia que se cree que tendrá un crecimiento exponencial en los próximos años, tal y como se ha mostrado en la introducción de esta sección, ante la que la seguridad es fundamental para lograr que la tendencia se materialice según las previsiones; y es que la falta de seguridad o de privacidad podría suponer una vía de inseguridad que podría ser utilizada por los ciberdelincuentes. Las aplicaciones relacionadas con el Internet de las cosas serán tan comunes en nuestra vida diaria, a veces de forma transparente, sin que los ciudadanos sean conscientes de ello, que mucha información sensible personal podría quedar al alcance de terceros si no hay una protección adecuada.

Así, en una situación en la que el Internet de las cosas se encuentre completamente desarrollado, los sensores de la casa mostrarán la hora a la que se levantan los miembros de la familia, al basarse en datos como el encendido de la calefacción o cuándo empieza a funcionar la máquina de café. Además, la monitorización del funcionamiento de los diferentes dispositivos permite obtener patrones sobre el número de personas que habitan en una vivienda y su comportamiento. Una vez fuera de casa, de camino hacia el trabajo, centro de estudios, u otras actividades, sensores de situación tanto de los vehículos como de otros dispositivos de carácter personal como el *smartphone* o *wearables* mostrarán la ruta, las paradas, con quién se está realizando el trayecto... Aún más, si se viaja en coche, los sensores de este mostrarán información sobre las configuraciones de conducción, sobre qué música se escucha...

Incluso si el usuario ha restringido sus datos, por ejemplo limitando su localización a la región en la que se encuentra —con lo que en teoría es difícil encontrar su localización exacta—, esto no es siempre verdad, y se pueden dar casos como que un usuario esté en un corto espacio de tiempo en tres regiones diferentes, lo que lo ubicaría con mucha exactitud, o que se combinen varios tipos de datos para mostrar su posicionamiento. Simplemente un dispositivo como el *smartwatch* puede suministrar información de quién eres, dónde estás, qué actividad estás haciendo e incluso el estado de ánimo.

Como se observa, todo un caudal de datos personales, de actividad, de preferencias; en definitiva, información que nos define y sobre la que el usuario empieza a querer tener un cierto control.

4.3.2 Soluciones de seguridad

Como se muestra, el Internet de las cosas implica un cambio del concepto de Internet, que pasaría de ser un entorno exclusivo para las personas, a poseer un carácter global en el que las cosas también formen parte de él. Esto supone el rediseño de todos los elementos que forman parte de la cadena de prestación del servicio, desde el *hardware* hasta las redes inalámbricas.

Una iniciativa de gran calado, que significa la redefinición de Internet casi desde el principio, y que lleva asociado un desafío enorme desde el punto de vista de la seguridad. Al igual que sucede con otros procesos de la sociedad de la información, será necesario que se sigan los siguientes cuatro principios básicos de seguridad: (1) resiliencia ante los ataques, que ante el ataque de un nodo concreto de la red, la seguridad global no se vea comprometida; (2) autenticación de los datos, que al igual que las personas, garanticen que los objetos son quienes dicen ser; (3) control de acceso que permita controlar de una forma ordenada qué objetos se conectan y si tienen derecho a conectarse; (4) privacidad del cliente, que mantenga unos estándares de privacidad acordes con la legislación y con los deseos y necesidades de los clientes potenciales.

En cuanto al Internet de las cosas, estas medidas mínimas con respecto a la seguridad se encuentran con algunas dificultades propias de tener que trabajar con infinidad de dispositivos, en muchas ocasiones de bajas prestaciones, a los que hay que añadir prestaciones de seguridad sin restar funcionalidad y aprovechando al máximo los recursos:

- Aprovechar los recursos de dispositivos pequeños, de poca potencia, al aire libre, con poca batería... para poder realizar las tareas esenciales manteniendo un mínimo de seguridad.
- Equilibrar que no se sacrifique la seguridad en favor de la eficiencia de estos dispositivos.
- Conseguir que se mantengan aislados aun estando conectados a la red principal, y no puedan comprometerlos.

Dado el alcance de este movimiento, así como sus características particulares que hacen que sea complicado mantener la robustez a lo largo de toda la red, se hace necesario tener en cuenta las cuestiones de privacidad y seguridad desde el mismo momento en el que se diseña. Al igual que sucede con otras tendencias como *big data*, es necesario diseñar los propios servicios pensando en la privacidad. Este enfoque es promovido por iniciativas como PbD (Privacy by Design)⁴⁴, que muestra los siguientes siete principios: (1) proactivo, no reactivo; preventivo, no correctivo, (2) privacidad como la configuración predeterminada, (3) privacidad incrustada en el diseño, (4) funcionalidad total: «Todos ganan», no «si

44. <https://www.privacybydesign.ca>

alguien gana, otro pierde», (5) seguridad extremo a extremo—protección del ciclo de vida completo, (6) visibilidad y transparencia—mantenerlo abierto, (7) respeto por la privacidad de los usuarios.

Se trata por tanto no solo de utilizar las tecnologías adecuadas, sino de situar la privacidad en el centro del proceso. En dicho proceso las tecnologías PET (*Private Enhanced Technologies*) jugarán un papel fundamental para que los servicios sean capaces de cumplir con los requisitos de seguridad que se requieren. Son tres los puntos fundamentales de actuación:

- Los datos comunicados por los dispositivos tienen que estar asegurados.
- La comunicación tiene que estar anonimizada.
- El almacenamiento de datos debe ser limitado para evitar la identificación de individuos.

Dada la importancia que la tendencia del Internet de las cosas está teniendo y sobre todo se espera que adquiera en los próximos años, es primordial que se desarrollen aplicaciones específicas que tengan en cuenta todos estos requisitos. En la actualidad ya existen soluciones como las aportadas por **Symantec**⁴⁵, que tienen en cuenta las particularidades de los dispositivos e incluyen analíticas de datos adaptadas a este entorno.

4.4 Internet industrial

El Internet industrial se puede considerar hasta cierto punto una extensión del Internet de las cosas. De hecho, es una tendencia denominada «Internet industrial de las cosas» en muchas ocasiones. Por ese motivo todos los aspectos de carácter general que se comentaron en el apartado anterior no solo se aplican en este apartado, sino que constituyen su base.

Si bien la conectividad de componentes, máquinas y dispositivos se ha explicado en la sección de Internet de las cosas, es la condición inicial para que se pueda producir este cambio de paradigma. Esta conectividad debe ser acompañada de otras innovaciones tecnológicas que permitan sacar el máximo provecho de la corriente de datos que se generen, darles sentido, integrarlas en el proceso de fabricación y utilizarlas con distintos fines.

En la actualidad, las tecnologías permiten la automatización de la actividad realizada por muchas de las máquinas de producción e incluso de procesos enteros. Esta automatización viene a significar que las máquinas puedan trabajar sin intervención humana pero sometidas a unas reglas muy estrictas. El reto consiste en dotar de cierta inteligencia a las máquinas de forma que puedan interactuar con el entorno de manera más autónoma y sean capaces

45. <https://www.symantec.com/iot>

de adaptarse a las situaciones y a los cambios directamente, sin que sea necesaria la intervención manual.

Es un proceso que se producirá en varias etapas:

- En una primera fase, que ya se ha alcanzado, puede dotarse a cada máquina por separado de capacidad para tomar ciertas decisiones o actuar de forma automática respondiendo así ante cambios del entorno. Por ejemplo, muchas máquinas tienen sensores que detectan condiciones del entorno y adaptan su producción.
- Posteriormente la inteligencia llega a la línea de producción, lo que supone que las máquinas deben comunicarse entre sí para poder adaptarse al ritmo de producción. Es una situación que ya se produce en los modelos de fabricación más avanzados y que da lugar a la fabricación flexible.
- La integración de líneas de fabricación inteligentes conlleva la fábrica inteligente. Uno de los ejemplos más conocidos es la factoría inteligente de Siemens, en Amberg (Alemania).
- En última instancia, se consigue ofrecer servicios inteligentes, lo que significa que estos serán capaces de adaptarse al entorno y de reaccionar de forma inteligente, comunicándose directamente con los usuarios y también con los proveedores.

Aunque como el nombre indica, el Internet industrial parte de la utilización masiva de Internet de las cosas en los entornos fabriles, debemos tenerlo en cuenta como una tendencia amplia, que requiere de la creación de ecosistemas para la prestación de servicios que son generalmente complejos y cuyo planteamiento se puede utilizar en diversos sectores económicos, como la logística, la salud o incluso la agricultura, como muestra la figura 4.1.

Figura 4.1 Aplicaciones de Internet industrial en el ámbito de la agricultura

365 FarmNet

Pioneer® Field360™ services

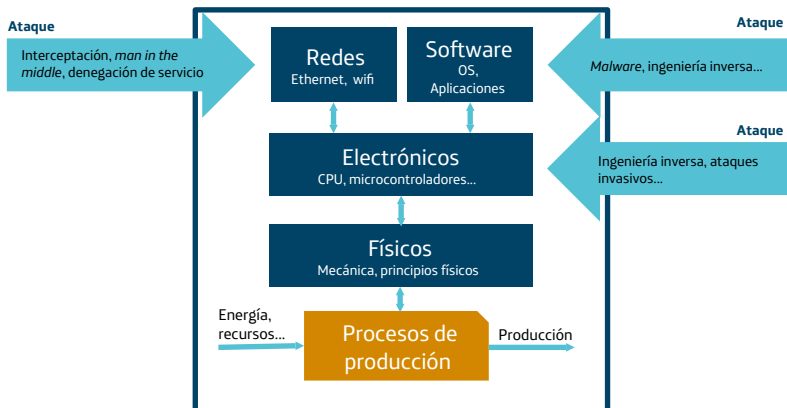
4.4.1 Necesidades de seguridad

La introducción de los conceptos y paradigmas propios de la computación en los entornos fabriles y otros entornos supone también la introducción de un gran número de tendencias tecnológicas como *big data*, computación en la nube o Internet de las cosas, tal y como se ha comentado anteriormente. Desde el punto de vista de la seguridad, en este campo aplican también las necesidades y soluciones de seguridad que se comentan en las secciones referentes a dichos temas.

Los ataques contra instalaciones industriales no son algo nuevo. Uno de los primeros casos que provocó la voz de alarma en este tema fue el gusano Slammer, que afectó al funcionamiento de dos sistemas críticos de monitorización de una planta nuclear en Estados Unidos en el año 2003. En los siguientes años se han sucedido ataques que han afectado a instalaciones industriales, aunque generalmente no eran ataques específicos hacia este tipo de instalaciones.

El aspecto fundamental del Internet industrial radica en la integración de los sistemas físicos tradicionales de producción con los sistemas computacionales que monitorizan dichos procesos en los que se han venido a llamar sistemas ciberfísicos (CPS). Este tipo de sistemas se pueden considerar el elemento base del Internet industrial y sobre los que deben desarrollarse medidas de seguridad propias. Si fuera una fábrica, que se podría tratar como un sistema ciberfísico de producción, las opciones de ataques afectan a las distintas capas, como las comunicaciones, el *hardware* y el *software*, además de los ataques a los propios empleados, como ocurre en cualquier otro entorno (ver la figura 4.2). La idea, por tanto, es proteger estas diferentes capas o superficies de forma que no existan debilidades en el sistema.

Figura 4.2 Tipos de ataque a los sistemas ciberfísicos de producción



Algún aspecto propio que se debe tener en cuenta también en el entorno industrial y en otros entornos económicos es la necesidad de disponibilidad de la maquinaria en todo momento, lo que condiciona las labores de mantenimiento y la posibilidad de que si algo falla, se produzcan accidentes en los que resulten heridas personas. En los servicios inteligentes, su carácter abierto y distribuido hace necesario un mayor control de los mecanismos de acceso.

4.4.2 Soluciones de seguridad

Las características propias que se han mostrado en la sección anterior muestran que son necesarias soluciones específicas para afrontar el desarrollo del Internet industrial. Dada la gran cantidad de particularidades: necesidad de disponibilidad, derechos de propiedad industrial, obligaciones legales de las empresas, posibilidad de accidentes físicos, entorno multinacional con diversas legislaciones... se requiere un enfoque holístico de las medidas de seguridad que deben mantenerse a lo largo de todo el ciclo de vida o el proceso productivo.

Además hay que pensar que la mayoría de las soluciones tradicionales de seguridad son muy pesadas para ser incluidas en los sistemas ciberfísicos. Lo más habitual en estos casos es el desarrollo de sistemas de *hardware* aislados de los sistemas críticos de seguridad y de los datos. Una solución es que las memorias de los sistemas sean solo de lectura, lo que facilita la seguridad, pero a cambio dificulta la actualización del sistema. Por ese motivo se han desarrollado sistemas que permiten actualizar la carga de funciones durante el arrancado del dispositivo o durante la ejecución.

Son necesarios también modelos de certificación para detectar la existencia de *software* malicioso o no deseado en el momento en que son muchos los dispositivos que se conectan. Aunque los más fiables son los que se encuentran embebidos en el *hardware*, es más económica su implementación mediante *software*. Cuando cientos de dispositivos se conectan automáticamente, se requieren mecanismos flexibles de certificación. Otro problema que surge es la propia gestión de miles de dispositivos, que además deben conectarse de forma sencilla y sin realizar actividades complejas sobre ellos.

Por todos estos motivos, los sistemas deben ser diseñados teniendo en cuenta la seguridad y testados atendiendo a certificaciones como la norma ISO/IEC TR/19791 de evaluación de la seguridad para sistemas operacionales o la serie de estándares de seguridad en sistemas de control ISA/IEC 62443. El aumento de la concienciación de la gravedad de las amenazas está favoreciendo el desarrollo de estos estándares de forma coordinada entre la industria y las Administraciones públicas, que son esenciales para el despliegue y correcto funcionamiento del Internet industrial en los diferentes sectores productivos.

El carácter central que tendrá la seguridad en el desarrollo del Internet industrial en las empresas deberá reflejarse también en la estructura de la empresa, por ese motivo será cada vez más necesario el papel de *Chief Security Officer*, encargado de coordinar las acciones relativas a la seguridad. Al igual que ocurre con la seguridad en otros ámbitos, una de las medidas más importantes que se debe aplicar es la formación de los empleados, siendo esta una de las herramientas clave para evitar riesgos por comportamientos no seguros. Así, tal y como se ha comentado anteriormente, la sensibilización y formación de todos los empleados respecto a estos temas será clave en el desarrollo del Internet industrial.

4.5 Apps móviles

El consumo de tecnologías por parte de los usuarios ha tendido hacia la movilidad por un lado y, por otro, hacia la utilización de aplicaciones, las conocidas apps, que han sustituido a los programas de *software* tradicionales. Los datos de utilización de las aplicaciones no han parado de crecer; en la actualidad, ya hay 1,5 millones de estas aplicaciones diferentes en la tienda Apple App Store y 1,6 millones en Google Play⁴⁶, números que no dejan de crecer.

De hecho, las apps constituyeron el uso preferido para conectarse desde los dispositivos móviles: el 90 % del tiempo de conexión a Internet a través de un dispositivo móvil se destina a su uso y cada mes se lanzan al mercado unas 40.000 nuevas apps⁴⁷. En España, en el año 2015, ha habido un total de 27,7 millones de usuarios de aplicaciones, que se descargaron 3,8 millones de aplicaciones diariamente. La media de aplicaciones por dispositivo es de treinta en los *smartphones* y de veinticuatro en las tabletas, de las que solo se utilizan de forma activa 14. Su uso en el móvil supera a la navegación y supone ya el 89 % del tiempo que se utiliza el móvil⁴⁸.

Aunque los usuarios las asocian generalmente al móvil y a la tableta, cada vez son más habituales en otros tipos de dispositivos como por ejemplo la televisión. También el *smart-watch* es un dispositivo muy propicio para la instalación y utilización de apps, lo que impulsará su desarrollo y el de interfaces por ejemplo de voz. El vehículo es otro entorno adaptado al uso de apps, como muestra el hecho de que en un estudio realizado entre fabricantes de vehículos en España, once de las quince marcas analizadas ya disponían de tienda propia de apps⁴⁹.

46. Statista. Datos de julio de 2015.

47. Informe Mobile en España y en el mundo 2015, Ditrendia.

48. 6.º informe sobre el estado de las apps en España 2015, TheAppDate.

49. IAB. I Estudio de Coches Conectados, datos de julio de 2014, datos de España.

4.5.1 Necesidades de seguridad

La capacidad de las apps de recolectar datos personales y de comportamiento continuamente las convierten en un foco de posibles fugas de información que afecten a la privacidad de las personas. Una de las principales dificultades para evitar esta situación e incluso para analizarla de una forma global reside en las diferencias regulatorias en los distintos países, todo ello en un modelo en el que los servicios tienen un carácter global.

No obstante, en la mayoría de las áreas del mundo se está imponiendo la tendencia de que las organizaciones recojan la menor cantidad posible de información sobre los usuarios para realizar su actividad, o la información de forma anonimizada y ofreciendo el control de los datos al usuario. Un ejemplo en este sentido es la inclusión de estos conceptos en las leyes regulatorias sobre privacidad recientemente aprobadas en China: «Cuando los operadores de telecomunicaciones o proveedores de servicios de Internet coleccionen o usen información personal de los usuarios, estos deben ser claramente informados de los propósitos, métodos y alcance del procesamiento, así como rectificar la información y las consecuencias de no suministrar dicha información»⁵⁰.

Existe, por tanto, un consenso respecto a la importancia de tener en cuenta la privacidad en el diseño de los distintos servicios. En concreto, en la legislación de Estados Unidos se menciona a las apps proponiendo «explicar qué información recoge tu app de los usuarios y sus dispositivos y qué hacer con sus datos»⁵¹.

En Europa⁵², la regulación también trata el asunto de la privacidad en el caso de las aplicaciones móviles y aborda temas como la falta de transparencia, la falta de consentimiento, las dificultades para entender las políticas de privacidad...

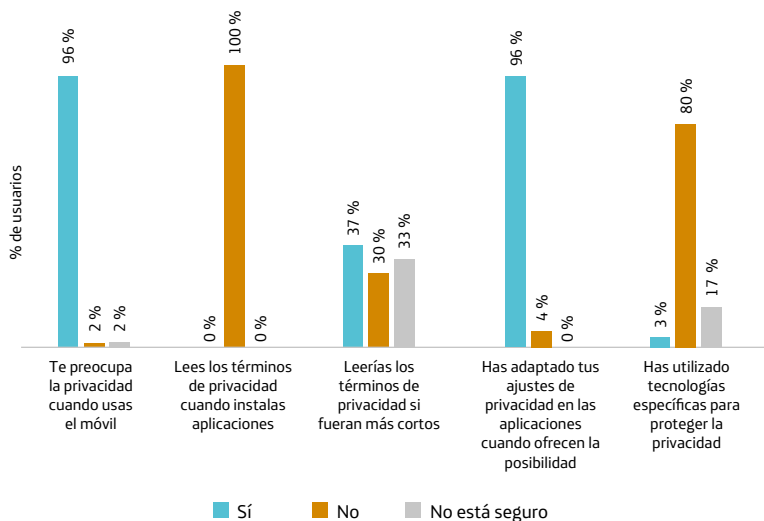
En la actualidad, las apps manejan estos problemas de privacidad mediante la obligación de que el usuario confirme que conoce la política de privacidad o los términos de consentimiento. Sin embargo, la experiencia muestra que no es una medida efectiva como refleja la figura 4.3.

50. Chinese Ministry of Industry and Information Technology concerning Telecommunication and the Internet Users' Personal Information Protection Regulation (2013).

51. Federal Trade Commission, Marketing Your Mobile App: Get It Right from the Start (April 2013).

52. Article 29. Data protection working party.

Figura 4.3 Actitud de los usuarios ante los términos de privacidad de las apps



Fuente: Shanghai University. Base: estudiantes universitarios entre 18 y 22 años.

Según dicha encuesta, los usuarios están preocupados por su privacidad, aunque el 100 % reconoce que no lee los términos de privacidad. Esta encuesta también muestra que un 72 % de los usuarios supone que una empresa va a realizar un tratamiento cauteloso de la información si acepta las políticas de privacidad, cuando en realidad muchas empresas no tienen siquiera una política de privacidad. Se refiere a una situación que debe ser gestionada para ofrecer soluciones que den tranquilidad a los usuarios, sobre todo teniendo en cuenta el crecimiento que se está produciendo en el uso de las apps y que se espera que continúe en el futuro.

4.5.2 Soluciones de seguridad

En la actualidad existen herramientas que facilitan la implementación de medidas de privacidad en los móviles, como 360 Mobile Safe⁵³, en China, o Niji, en España. No obstante, es este un tema en el que la acción más importante consiste en la concienciación de todos los agentes que participan en la cadena a la hora de prestar los servicios, ya que cada uno tiene una responsabilidad que es necesario que tenga en cuenta para que se garantice la privacidad a lo largo del proceso.

En primer lugar, las Administraciones deben continuar regulando en el sentido que lo están haciendo, y avanzar todavía más en facilitar el que los términos de privacidad se redac-

53. <https://play.google.com/store/apps/details?id=com.qihoo360.mobilesafe&hl=en>

ten en un lenguaje sencillo que pueda ser entendido por todos. Además, se deben evitar abusos en los que un usuario que actúa de buena fe se pueda ver comprometido en temas de privacidad.

Toda la cadena de desarrollo de las aplicaciones, desde los desarrolladores hasta las empresas que gestionan las tiendas, debe ser consciente de las necesidades de privacidad y ofrecer soluciones. Por ejemplo, un 99 % de los usuarios piensa que un sistema de *opt-in* de los distintos tipos de información que desean compartir, algo que ya incluyen ciertas redes sociales, ayudaría a gestionar mejor su privacidad.

El uso de mensajes emergentes cada vez que un tipo concreto de información va a ser compartida es otra opción que también ayudaría a que los usuarios tuvieran un mayor control de sus datos. Además de mostrar al usuario qué tipo de información está compartiendo, sería muy interesante que las aplicaciones explicaran por qué necesitan dicha información, si la información se ofrecerá también a terceras partes y a quién se cederá, cuáles son los derechos que el usuario tiene y cómo retirar sus datos.

Por último, los usuarios deben ser conscientes de los problemas de privacidad y seguridad que se encuentran asociados a su actividad. Deben ser capaces de renunciar a funciones determinadas si creen que su uso significa una sobrexposición en los medios de Internet y también deben ser exigentes primando las aplicaciones que les facilitan el control de los datos.

4.6 Múltiples identidades digitales: el reto para protegerlas e identificarlas con la identidad física

Según lo que se ha comentado en el primer capítulo, el concepto de identidad tiene una relación importante con el contexto y las circunstancias; por ejemplo, una persona puede ser, en función del contexto, padre, abogado, diabético, propietario de una vivienda y socio del Real Valladolid; factores de la identidad que tienen sentido en entornos determinados. También puede juzgarse la identidad desde el punto de vista pragmático, siendo en ese sentido la capacidad de identificar a un individuo y de identificar los servicios a los que tiene derecho.

Ante esta situación de diversidad de identidades o al menos de diferentes aproximaciones del significado de identidad, las Administraciones tienen en el poder identificar de forma unívoca a los diferentes ciudadanos su mayor necesidad. Al igual que sucedía con los temas analizados anteriormente, se trata de un aspecto de gran importancia, que debe ser tenido en cuenta de una manera global, sopesando tanto la vertiente legal como la tecnológica.

4.6.1 Necesidades de seguridad

Como se ha comentado, el tema de las identidades es complejo, tanto conceptualmente como desde el punto de vista tecnológico. Esta complejidad viene dada por el hecho de que la identidad no se puede considerar un elemento único que define a la persona, sino que siempre es un concepto que se encuentra fragmentado, y que aparece como la suma de varias partes. En el caso de la identidad digital, esta fragmentación es todavía más patente. Esta situación en la que la información se halla dispersa en diferentes lugares, muchas veces sin que seamos capaces de relacionarlos, y donde muchos agentes pueden intervenir, es la causa fundamental de la complejidad de controlar la información. Por ejemplo, un usuario no tiene la intención de subir fotos suyas a Internet, pero un conocido puede subirlas y etiquetarlas, de forma que estas acciones afectan a su identidad sin él saberlo.

El hecho de que sean muchas las entidades que están relacionadas de una u otra forma con nuestros datos y que generan información sobre los usuarios incluso en forma de metadatos (datos de nuestros datos) hace que sea muy difícil controlar el ciclo de vida de los datos de principio a fin. El abaratamiento de los costes de almacenamiento supone que cada vez es posible que un mayor número de entidades graben la vida online de los internautas y que después esta vida online se pueda convertir en conocimiento tras un análisis profundo. Los avances en tecnologías como *big data* añaden nuevas capacidades y juegan un papel cada vez más relevante para obtener el máximo beneficio de estos datos. Además de las entidades relacionadas directamente con los datos, han aparecido otras que actúan como brókeres que comercian con ellos y los suministran después a organizaciones que puedan estar interesadas, con lo que los datos se pueden estimar como el «nuevo dinero».

Por todos estos motivos, los fraudes relacionados con la identidad son muy diversos. Un ejemplo muy típico es el de buscar información en diferentes partes de Internet para sustituir a un usuario y realizar actividades ilícitas en su nombre. En estos casos, la sustitución de las interacciones físicas por interacciones online facilita la actividad de los delincuentes.

La utilización de forma agregada de datos que se encuentran de forma fraccionada en la web creando perfiles de usuarios también tiene posibles efectos sobre estos. Además es una actividad fácil de realizar teniendo las tecnologías disponibles actualmente. De hecho, en ocasiones no supone gran complejidad técnica; por ejemplo, un estudio publicado en el año 2013 mostraba que es fácil sacar información sensible de los usuarios simplemente analizando los *likes* de Facebook⁵⁴. Las discriminaciones basadas en dichos perfiles, por ejemplo, por parte de aseguradoras, de empresas empleadoras, pueden suponer un pro-

54. Kosinski, M., Stillwell, D., & Graepel, T. (2013), «Private Traits and Attributes Are Predictable from Digital Records of Human Behavior», *Proceedings of the National Academy of Sciences*, 110: 15, p. 5802.

blema para muchos usuarios. Además, diversos estudios muestran que es posible utilizar estos datos para predecir comportamientos; por ejemplo, un estudio concluye que es posible predecir con ellos nuestra localización con ochenta semanas de antelación y un 80 % de fiabilidad⁵⁵.

Otro tema de especial relevancia relacionado con la identidad digital es la capacidad de conectar la identidad física de una persona con su identidad digital. Muchas veces el problema es que se pueda producir un error y una tercera persona física se aproveche por ejemplo de una transacción u otra actividad realizada en Internet. Otras, el problema es el contrario, que la mezcla de información de diferentes sitios online e incluso con información de sitios offline sea capaz de identificar a una persona que no desea ser identificada, al menos con ciertas actividades realizadas de forma digital.

4.6.2 Soluciones de seguridad

Como se ha mostrado a lo largo de la sección, la identidad es un tema complejo que afecta a todos los eslabones de la prestación de los servicios y a los usuarios. Se requiere un enfoque global en el que se definan claramente aspectos como cuáles son los límites que se deben poner a la recogida de datos, su tratamiento, su utilización, los derechos de los usuarios en cuanto a su control... jugando la regulación un papel central en su definición y evolución. No obstante, las soluciones tecnológicas serán necesarias para implementar una gestión de la identidad que tenga en cuenta dichos aspectos, aunque debe aclararse que no existe una solución que abarque todos estos temas ni que sea capaz de abordarlos en todos los entornos, dado el modelo fragmentado de Internet. La internacionalización de los servicios y la dificultad de evitar el movimiento entre fronteras supondrá un desafío añadido para la implementación de cualquier solución en la gestión de la identidad.

En el apartado anterior hemos definido dos tipos de problemas relacionados con la identidad. Por una parte, la gestión de cantidades ingentes de información relativas a los internautas que se generan continuamente en un sistema tan fragmentado como es Internet y que pueden ser utilizadas por terceros de forma inadecuada; por ejemplo, discriminando a los usuarios, o incluso haciéndose pasar por ellos. Por otra parte, la dificultad de relacionar la identidad digital y la identidad física, aspecto que es necesario en muchos servicios y en las relaciones con la Administración.

Con respecto a la primera situación, son muchas las aplicaciones e iniciativas que se han desarrollado para facilitar el anonimato en la red, como Anonymizer.com⁵⁶ o Tor Project⁵⁷. Tam-

55. http://www.cs.rochester.edu/~sadilek/publications/Sadilek-Krumm_Far-Out_AAAI-12.pdf

56. <https://www.anonymizer.com>

57. <https://www.torproject.org/index.html.en>

bién se intenta que la información que queda libre en las distintas interacciones con los servicios sea la menor posible, tal es el objetivo de la tecnología criptográfica U-prove⁵⁸ de Microsoft o Identity Mixer⁵⁹ de IBM.

No obstante, son soluciones parciales que se centran en alguna tarea o proceso concreto, pero que no tienen en cuenta toda la interacción del usuario en la red. Por ello se están realizando proyectos que muestran una aproximación holística al concepto de identidad, como es el proyecto SuperIdentity⁶⁰, en el que participan diversas universidades y organizaciones y que estudia los diferentes aspectos de la identidad digital, de la identidad física y de las interrelaciones entre ambas. Otro aspecto fundamental que está relacionado con la identidad y que se ha descrito anteriormente es el control de la información personal por parte de los usuarios. A este respecto, el proyecto Midata⁶¹, en el Reino Unido, es una iniciativa para que los usuarios sean capaces de acceder a los datos que las empresas y otras organizaciones tienen sobre ellos.

Respecto al segundo problema, la necesidad que tienen muchos servicios y organizaciones de asociar una identidad digital con una identidad física, se recurre a ciberidentificadores que tratan de asegurar que la persona física es la que tiene derecho a utilizar un servicio determinado online. Los mecanismos utilizados son nombres de usuario, contraseñas, PIN, análisis de los hábitos de navegación, preguntas personales... Para mejorar la seguridad se han empezado a utilizar mecanismos redundantes como realizar preguntas y además utilizar algo que el usuario tenga, como el teléfono móvil. Así, cada vez es más frecuente que se requiera a los usuarios a la hora de hacer transacciones, además de la contraseña, un código que se envía a su teléfono móvil.

También esta es la filosofía que se encuentra detrás del servicio Mobile Connect⁶², una iniciativa de los operadores globales de telecomunicaciones GSMA que tiene como objetivo incrementar la seguridad en el manejo de la identidad y la privacidad en Internet, para lo cual utiliza el teléfono móvil como elemento de identificación. Este enfoque parte de la realidad de que la mayoría de los internautas dispone de teléfono móvil (ya existen tantos teléfonos móviles como personas en el planeta), un dispositivo que se utiliza de forma personal, y además la mayoría de los usuarios lo tiene a su alcance en todo momento. Mobile Connect utiliza el móvil para conectarse a los diferentes servicios online de forma que se evita que el usuario tenga que utilizar diferentes claves para acceder a diferentes servicios, situación que es complicada de gestionar y que da lugar a gran cantidad de errores y fugas de seguridad.

58. <http://research.microsoft.com/en-us/projects/u-prove>

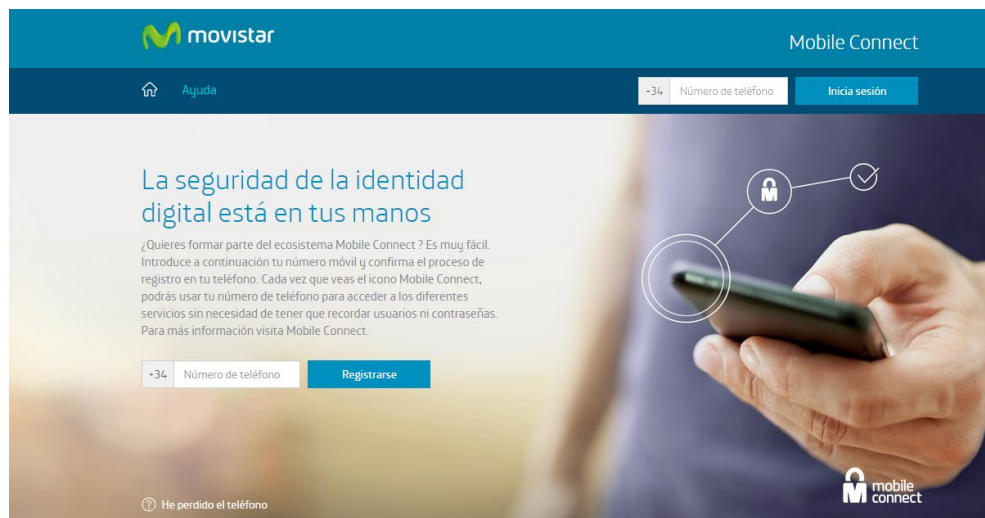
59. <http://www.zurich.ibm.com/idemix>

60. <http://www.southampton.ac.uk/superidentity/index.page?>

61. <https://www.gov.uk/government/news/next-steps-making-midata-a-reality>

62. <http://www.gsma.com/personaldata/mobile-connect>

Figura 4.4 Versión Mobile Connect de Movistar



[Conoce más acerca de Mobile Connect](#)

Además de estos planteamientos, la utilización de variables biométricas como la huella digital, el iris o el análisis de rostro se muestran como un gran avance en el objetivo de conectar a los usuarios digitales con los usuarios físicos. Se trata, además, de una forma segura —los rasgos biológicos son individuales e intransferibles— que ya está siendo utilizada por diversos servicios.

Esta enumeración de soluciones refleja la complejidad de abordar la identidad digital. Parece claro que dada la naturaleza de este tema, el diseño de los sistemas teniendo en cuenta desde el principio todas las cuestiones relativas a la identidad y privacidad es la mejor manera de abordar esta cuestión de una forma global. También la concienciación de los usuarios de los aspectos asociados a la identidad y sus implicaciones es fundamental para prevenir los posibles problemas relacionados con este tema.

4.7 Desafíos legales de la ciberseguridad

El reforzamiento de la ciberseguridad no solo presenta desafíos tecnológicos. Una regulación adecuada y la existencia de mecanismos legales adaptados a los avances tecnológicos son fundamentales en la lucha contra el ciberdelito. De los desafíos analizados en los apartados anteriores, dos son los que más relevancia tienen desde un punto de vista legal, dada su rápida expansión y su relación con la generación, transmisión y custodia de información a través de las redes de comunicación: la prestación de servicios de *cloud computing* y el desarrollo de soluciones IoT.

Como ya sucedió en el pasado con otras innovaciones tecnológicas, surgen también dudas normativas o regulatorias relacionadas con la seguridad e integridad de la información almacenada, especialmente de la que pueda tener naturaleza más sensible por su carácter confidencial o por tratarse de datos de carácter personal especialmente protegidos por la normativa de aplicación (recogida para España en la Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal⁶³ y su normativa de desarrollo, Real Decreto 1720/2007 de 21 de diciembre⁶⁴), más las numerosas resoluciones (normas de carácter reglamentario) dictadas por la Agencia Española de Protección de Datos (AEPD).

En el seno de la Unión Europea son de aplicación las directivas comunitarias sobre protección de datos (Directivas 95/46/CE y 2002/58/CE), traspuestas por los distintos Estados miembros a sus respectivas legislaciones nacionales. Esta armonización normativa permite a cualquier usuario acudir a los servicios de almacenamiento de información de un proveedor de *cloud computing* que tenga sus centros de proceso de datos ubicados en la Unión Europea, sin temor a que las obligaciones en materia de protección de datos se vean incumplidas. Estas contemplaciones son extensivas a los Estados cuyas normativas en la materia se equiparan a la europea, así como a aquellos proveedores radicados en Estados Unidos que son tratados como *safe harbour* (puerto seguro), por adherirse voluntariamente a este protocolo, en virtud del cual se obligan a cumplir requisitos equivalentes a los europeos en materia de protección de datos. La Agencia de Protección de Datos mantiene en su página web una relación de países cuya regulación en la materia se considera equiparable a la europea⁶⁵.

En relación con el tratamiento de la información en servicios de *cloud computing*, es necesario recordar que no todos los datos de carácter personal gozan del mismo nivel de protección. El artículo 7 LOPD establece la existencia de datos especialmente protegidos, entre los que se encuentran por ejemplo los relativos a salud, orientación sexual, ideología o religión, para los que las medidas de protección que debe adoptar el encargado del tratamiento del fichero son especialmente rigurosas. Así, los artículos 79 y siguientes del RD 1720/2007, por el que se aprueba el Reglamento de la LOPD, establecen tres niveles de seguridad (básico, medio y alto) que se asocian a tres categorías de datos en función del nivel de protección de los mismos. Es obligación del encargado del tratamiento articular las medidas necesarias para dotar a los datos del nivel de seguridad correspondiente; y corresponde al responsable del fichero exigir a su proveedor de servicios *cloud* que articule dichas medidas. Los artículos 89 y siguientes del RD 1720/2007 desarrollan cuáles son las medidas exigibles al encargado del tratamiento para cada nivel de seguridad de los datos.

63. http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Ley_Organica_15-1999_de_13_de_diciembre_de_Proteccion_de_Datos_Consolidado.pdf

64. http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs/2014/Real_Decreto_1720-2007_de_21_de_diciembre_por_el_que_se_aprueba_Reglamento_de_desarrollo_Ley_Organica_15-1999_Consolidado.pdf

65. http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php

También es importante recordar que de conformidad con la normativa española de protección de datos, el usuario, a efectos de tratamiento de los datos de carácter personal, tiene la distinción de responsable del fichero, y el proveedor, el de responsable del tratamiento, con lo que ello trae consigo a efectos de responsabilidades jurídicas. Por tanto, son comprensibles también las lógicas reservas por parte de los usuarios a perder el control físico de datos personales, confidenciales, sensibles o reservados, tanto si se refiere a los suyos propios como de los de sus clientes si se trata de una empresa, en la medida en que estos datos dejan de estar en los servidores de su propiedad o en discos o dispositivos que se guardan en un lugar físicamente seguro y que se encuentra, en último extremo, bajo el control del usuario y dentro del ámbito territorial competencial de un Estado determinado.

Los riesgos normativos en el modelo de *cloud computing* se concretan en que los datos pasan a encontrarse en algún lugar indeterminado, en un servidor cuya ubicación física puede incluso llegar a desconocerse por el usuario. ¿Cuál es entonces la normativa aplicable? ¿Qué ocurre si hay alguna vulnerabilidad? ¿Qué garantías jurídicas existen?

Hay tres aspectos esenciales que conviene tener en cuenta al hablar de los riesgos regulatorios en la contratación de los servicios de *cloud computing*:

- La seguridad y confidencialidad de los datos.
- La territorialidad y jurisdicción aplicable en caso de conflicto.
- Aspectos esenciales del contrato de servicios que deben firmarse entre usuario y proveedor, tanto desde el punto de vista técnico como jurídico.

La intención es determinar cuáles son las garantías jurídicas de que dispone el usuario tendente a asegurar que la información no se va a perder o a corromper en la nube y que ninguna persona no autorizada va a disponer de acceso a esta información. Además, lógicamente hay que establecer las oportunas garantías jurídicas de que el usuario quedará indemne frente a los perjuicios que se le pueden ocasionar a él o a sus clientes.

La solución a los potenciales problemas de seguridad en la prestación de servicios *cloud* pasa, entre otras acciones, por el reforzamiento de las garantías legales de los contratos, que han de incorporar, por mandato legal, las previsiones necesarias para garantizar el adecuado cumplimiento de la normativa relativa a la protección de datos.

En ese sentido y en el ámbito nacional, la propia LOPD establece en su artículo 12.2 que «la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni si-

quiera para su conservación, a otras personas. En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta ley que el encargado del tratamiento está obligado a implementar».

Los aspectos esenciales desde el punto de vista contractual a tener en cuenta son los siguientes⁶⁶:

- El proveedor de servicios *cloud* ha de garantizar la conservación de los datos, mediante la realización de copias de seguridad periódicas y dotando a su infraestructura de los mayores niveles de seguridad física y lógica.
- El proveedor ha de establecer mecanismos seguros de autenticación para el acceso a la información. Estos mecanismos han de permitir la compartición e intercambio de información sin que sea posible que personas no autorizadas accedan a información reservada o confidencial.
- El cifrado de los datos almacenados es una necesaria medida de seguridad. El usuario ha de conocer el nivel de seguridad ofrecido por las técnicas de cifrado de la información que aplique en sus sistemas.
- Es fundamental disponer de un procedimiento de recuperación y migración de los datos a la terminación de la relación entre el usuario y el proveedor; así como el mecanismo de borrado de los datos por parte del proveedor una vez que estos han sido transferidos.
- La propia naturaleza del modelo *cloud computing* hace posible que, en principio, los datos almacenados en la nube se encuentren físicamente en un servidor ubicado en cualquier punto del planeta, lo que ha de ser tenido en cuenta si se utiliza el servicio de almacenamiento para conservar datos de carácter personal.

Desde el punto de vista de las garantías jurídicas, la muy probable circunstancia de que los datos no se almacenen en territorio español plantea la fundamental cuestión de qué ocurre cuando estos están almacenados en otro país en el que la LOPD carece de fuerza legal. La Directiva 95/46/CE contempla en su artículo 25 la transferencia de datos personales a países terceros⁶⁷ y señala que la transferencia debe limitarse a naciones en las que los datos cuenten con lo que se define como «un nivel de protección adecuado»⁶⁸. En cuanto a la legis-

66. Consejo General de la Abogacía: «Utilización del cloud computing por los despachos de abogados y el derecho a la protección de datos de carácter personal» http://www.abogacia.es/wp-content/uploads/2012/07/informe_CLOUDCOMPUTING.pdf.

67. http://europa.eu/legislation_summaries/information_society/l14012_es.htm, aunque hay que tener en cuenta que el texto está siendo objeto de procesos de revisión dirigidos a actualizarlos para tener en cuenta las consecuencias de los desarrollos tecnológicos, la globalización de los intercambios de datos y, en el caso de la Directiva, las modificaciones legales e institucionales que supuso la entrada en vigor en 2009 del Tratado de Lisboa. La Comisión presentó en enero de 2012 dos propuestas de nuevos actos normativos. Un Reglamento General de Protección de Datos y una Directiva de protección de datos en materia de cooperación policial y judicial. Ambos textos se están tramitando en el procedimiento legislativo ordinario, con participación del Consejo y el Parlamento Europeo.

68. La Agencia Española de Protección de Datos (AEPD) informa de los países con un nivel de protección adecuado en su página web: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php

lación nacional, el denominado movimiento internacional de datos está regulado en la LOPD en sus artículos 33 y 34. Por tanto, a la hora de analizar las implicaciones legales de la contratación de servicios *cloud*, es necesario distinguir dos supuestos: cuando en el país en el que se ubiquen los datos exista una legislación equiparable a la europea que garantice un adecuado nivel de protección (entonces los riesgos jurídicos son lógicamente mucho menores) y cuando no ocurra así (en el que los riesgos jurídicos aumentan notablemente).

Para el segundo supuesto hay que tener en cuenta que si el proveedor almacena sus datos en un país cuya normativa de protección de datos no es equiparable a la europea, se requiere la autorización previa de la Agencia de Protección de Datos para que el responsable de un fichero de datos de carácter personal encargue su tratamiento a una persona o empresa que reside fuera del espacio de legislación armonizada o equiparada. Por otro lado, es importante destacar que el contrato de provisión de servicios ha de incorporar cuantas condiciones sean necesarias para suplir la carencia de la legislación, al trasladar al encargado del tratamiento del fichero las mismas obligaciones que contempla la normativa europea. Para la elaboración de este tipo de acuerdos pueden tomarse como referencia las *standard contractual clauses for the transfer of personal data to third countries*⁶⁹, elaboradas por la Comisión Europea y que garantizan una adecuada protección en la transferencia de información de carácter personal a terceros países. Es importante resaltar que el responsable del fichero, es decir, el usuario, es el responsable de seleccionar como encargado del tratamiento del mismo a alguien que verifique los requisitos legalmente establecidos.

En relación con el desarrollo de servicios IoT, los requisitos de seguridad que se están definiendo de facto en la industria empiezan a ser recogidos por las legislaciones. Por ejemplo, en la Unión Europea, estos requisitos están integrados en la regulación de protección de datos. En Estados Unidos, este tipo de regulación se aplica solamente a ciertos tipos de datos, como por ejemplo la información médica mediante la HIPAA (*Health Insurance Portability and Accountability Act*).

En este entorno, la Declaración de Mauricio del 14 de octubre de 2014 sobre Internet de las cosas y firmada por cien países propone que la transparencia es un aspecto al que debe darse tanta importancia como a la privacidad, de forma que los usuarios tengan el control de sus datos.

Además de los enfoques técnicos para asegurar la privacidad y la transparencia, se imponen otras normas generales como la minimización de información, que es un principio fundamental en la legislación europea, de tal manera que los datos se conserven agregados y solamente durante el tiempo necesario. Otra opción es la perturbación que supone que los datos se alteran sistemáticamente mediante una función o la ofuscación que supone que ciertos datos se reemplazan por valores aleatorios.

69. Decisiones 2004/915/EC, 2001/497/EC, y 2002/16/EC de la Comisión Europea.

Transcripción del encuentro de expertos en ciberseguridad

Reunión de expertos en ciberseguridad	72
Introducción	73
Miguel Pérez Subías	77
Paloma Llaneza	81
Elena García Díez	87
Manuel Escalante García	95
Carlos Abad Aramburu	103
José Valiente	111
Antonio Guzmán	117
Ángel León Alcalde	123

Reunión de expertos en ciberseguridad

Para la realización de este informe sobre ciberseguridad, Fundación Telefónica ha contado con la colaboración de un grupo de expertos que se reunió el 25 de febrero de 2016 para debatir y compartir sus impresiones y conocimiento sobre la materia. Este apartado recoge la transcripción literal de las intervenciones de los expertos durante dicha reunión. Cada experto intervino individualmente para compartir su punto de vista sobre un borrador del estudio y dio respuesta a una serie de preguntas sobre cada una de sus áreas de especialidad. Posteriormente se abrió un turno de debate entre todos los participantes.

Imagen 5.1 Grupo de expertos en el debate sobre ciberseguridad



Introducción



ANTONIO CASTILLO

Moderador del debate

En primer lugar, daros la bienvenida y agradeceros la disponibilidad para participar en este ejercicio. Esta reunión es una práctica habitual que llevamos realizando desde 2009. Hacemos dos debates anuales sobre temas que estén de actualidad y sean pertinentes desde el punto de vista tecnológico. Tiene que ser un asunto que produzca un impacto social y económico y del que se esté hablando de forma generalizada en la sociedad. Nuestro objetivo es aportar luz sobre esa materia en cuestión. También se pretende que sea un documento donde los expertos como vosotros os sintáis cómodos, pero fundamentalmente va dirigido a un público interesado pero no experto.

Hemos intentado traer a expertos sobre tres temas fundamentales a los que queremos dar respuesta. El primero es la percepción de los usuarios sobre la ciberseguridad. También nos interesa saber el impacto que va a tener sobre la industria y la competitividad de nuestro país y, en general, sobre la actividad económica a escala global. Por último, cómo se ve en el futuro, desde un punto de vista tecnológico y de aplicación.

En este documento, como hemos dicho, hemos tratado de abordar el tema desde el punto de vista de los usuarios en distintos aspectos. Uno es desde la percepción de los usuarios de Internet. Por eso Miguel Pérez Subías está aquí: es el presidente de la Asociación de Usuarios de Internet. También contamos con Elena García Díez, de INCIBE, institución que vela por la ciberseguridad en España, y con Paloma Llana, que es nuestra abogada de cabecera en estos temas y socia directora de Razona Legaltech. En representación del sector industrial nos acompaña Indra, de la mano de Manuel Escalante. Carlos Abad, de Ikusi, empresa de seguridad tradicional, ofrece soluciones de seguridad electrónica para infraestructuras de alta relevancia, como aeropuertos, y de repente se encuentra en la necesidad de integrar la ciberseguridad entre sus soluciones. También destacamos la presencia de José Valiente, del Centro de Ciberseguridad Industrial, y de Ángel León Alcalde, representante del Ministerio de Industria.

Primero, Javier Carbonell, de Telefónica I+D, va a realizar una pequeña presentación del informe que han elaborado sobre este tema.



JAVIER CARBONELL

Telefónica I+D

Este informe se realiza porque Internet y las tecnologías digitales nos envuelven completamente. En la actualidad es prácticamente imposible mantenerse a su margen. En todos los ambientes de nuestra vida cotidiana — el ocio, el trabajo, las comunicaciones, etc.— el contenido digital se encuentra presente, lo que hace que la información se pueda grabar, reproducir y, cómo no, también escapar de nuestro control, caer en las manos de quien no debe e incluso ser utilizada en contra de nuestros intereses.

Existe un consenso generalizado entre la población de que las tecnologías hacen mucho por nosotros, aunque también la gente empieza a ser consciente de que pueden llegar a suponer un problema, al menos para algunos de nuestros valores fundamentales. Durante los últimos años ha sido más habitual de lo que debiera el que información sensible haya escapado del ámbito de los usuarios y de las empresas, lo que ha generado una alarma muy relevante. Según muestran estudios internos, la gran mayoría de los internautas, en concreto el 82,8 %, dan al tema de la seguridad una gran importancia. Y consideran que se debe proteger no solo sus datos personales y fotografías, sino otra información como el historial de búsquedas o el de navegación.

A la mayoría de los usuarios les gustaría poder controlar su vida digital, esto es, identificar y borrar los datos personales o ser capaces de moverlos entre diferentes plataformas. Parece entonces que hay una gran brecha entre lo que los usuarios desean y prefieren y la cruda realidad, en la que la mayoría de las plataformas son cerradas, utilizan los datos del usuario como una mercancía más y lo mantienen cautivo. Nos encontramos, además, en un momento muy importante, en el que más que una evolución de las tecnologías, estamos asistiendo a una verdadera revolución; un momento en que nuevas innovaciones y tendencias tecnológicas están tensionando todavía más los aspectos relacionados con la seguridad y la privacidad. Y es que muchas de las tendencias tecnológicas que marcan el desarrollo de la sociedad de la información suponen un gran número de desafíos frente a los cuales no podemos permanecer inmóviles.

El Internet de las cosas y más en concreto el Internet industrial provocarán que el número de objetos conectados a Internet crezca exponencialmente, desde nuestra ropa hasta los electrodomésticos de nuestra casa, lo que creará todo un torrente de información que debe ser controlado para evitar que nuestra sociedad se convierta en un Gran Hermano.

La computación en la nube tendrá como consecuencia el que la computación y el almacenamiento de datos se produzcan en lugares muy diferentes de donde se usan; en muchos casos, en la otra punta del mundo, con los consiguientes problemas de choques de legislaciones.

La movilidad y utilización masiva de apps también generan una corriente continua de datos, entre los que se incluye la geolocalización, que una vez analizados con técnicas *big data* pueden suponer problemas importantes para la privacidad de los usuarios.

También se detecta una convergencia entre los dispositivos utilizados por los usuarios en sus entornos personales y sus entornos profesionales, tendencia que se conoce genéricamente como BYOD (*Bring Your Own Device*), que puede llegar a suponer un agujero de seguridad en las empresas y ser un desafío importante para el Departamento IT. Esta situación no solo afecta a dispositivos, ya que muchos usuarios utilizan en el trabajo aplicaciones personales, a pesar de que la empresa dispone de aplicaciones específicas seguras para dichos fines, lo que se denominaría BYOA (*Bring Your Own Application*) o «efecto Dropbox».

Nos encontramos ante una encrucijada en la que parece que la previsión de evolución de la sociedad de la información choca con los deseos y necesidades de la población, y todo el mundo reconoce que en esta situación los modelos actuales de seguridad no valen. Nos referimos a un aspecto que debe abordarse de una manera global por todos los agentes que participan en la construcción de la sociedad de la información para que su desarrollo alcance su potencial en los próximos años.

El objetivo de este monográfico y de este *think tank* es poner en relieve esta circunstancia y fomentar el diálogo multidisciplinar en un tema tan importante para el futuro de las tecnologías como este.

Antonio Castillo

Después de la presentación del informe, vamos a comenzar con la intervención de Miguel Pérez, presidente de la Asociación de Usuarios de Internet. Creo que puede proporcionar grandes aportaciones porque, ahora mismo, hemos pasado de la sensación de que Internet era la panacea y nos arreglaba todo, a descubrir que no es un entorno tan seguro.



MIGUEL PÉREZ SUBÍAS

Presidente de la Asociación de Usuarios de Internet

Preguntas a partir de las cuales se inició su intervención:

- ¿Qué percepción tienen los usuarios de la seguridad en los servicios digitales?
- ¿Qué están haciendo los usuarios para protegerse?

Yo quizá voy a ser un poco disruptivo. En general, al usuario no le importa la seguridad ni la privacidad. Esa es la realidad. Imaginad que vosotros fuerais a un centro comercial y que tuvierais que pensar que os tenéis que poner un chaleco antibalas para evitar a un posible francotirador o que os tenéis que atar la cartera con una cadena para que no os la roben. La ciberseguridad tiene que ser algo intrínseco que genere confianza. Mientras estemos pensando que el usuario tiene que hacer algo o tiene que estar preocupado, es que el sistema no está funcionando adecuadamente. Eso quiere decir que se acepta en tanto en cuanto no se pierda la relación de confianza. La gente confía y somos así, confiamos. Pensamos que el sistema es seguro. De modo que la ciberseguridad es importante, pero en tanto confíe en el sistema no debería dársele importancia. De hecho, no se le da en las encuestas que se hacen. Es más, nos instalamos infinidad de aplicaciones en nuestros teléfonos que nos piden todos nuestros datos y se los damos (yo incluido).

¿Cuál es la percepción que tengo? Creo que hay una confianza excesiva en el sistema. Por otro lado, pienso que el enfoque es erróneo. Es erróneo porque mezclamos varios temas que deberían estar separados. Un fallo en la seguridad te puede afectar a la privacidad. Pero en este momento nuestro cuestionamiento de la privacidad se basa fundamentalmente en aplicaciones legales con las que aceptamos y permitimos que entren en nuestro correo electrónico, que accedan a nuestra información y nos pongan publicidad. Tenemos un cambio de valores. Si nos hubiesen preguntado si nos podían abrir nuestro correo postal, miraran qué hay en él y, en función de eso, nos pusieran en su interior un panfleto de publicidad, habríamos puesto el grito en el cielo. Pero esto ha cambiado en un entorno digital. Lo hemos

aceptado. Hemos perdido libertad en aras de un hipotético mejor servicio. Todos lo valoramos en positivo, o casi todos. La gente suele pensar «¡Qué bien que me voy a Milán y me llega publicidad sobre hoteles en Milán!» o «¡Qué bien que me gusta la fotografía y me llegan anuncios sobre fotografía!».

Por ello, el segundo aspecto relevante para mí es que seguridad siempre tiene que haber y tiene que funcionar bien. Es verdad que entonces es un continuo ir contra las aplicaciones, pero es cierto que en la privacidad estamos en un momento de cambio de paradigma. Teníamos un enfoque en el que el responsable de los datos era el que coge los datos. Esto está cambiando y, desde nuestro punto de vista, los datos deberían ser nuestros, no del que los recoge. Esto no es una realidad hoy. Los datos son del que los recoge o del que los puede recoger, y aun así no son de todos los que los recogen. Hay algunos que no pueden utilizarlos. Telefónica sería un caso. Esto afecta al enfoque del estudio, y yo haría una separata de la privacidad y la metería en un apartado aparte, porque además juega con el hecho de que si usted quiere cosas más seguras, tiene que renunciar a cierta privacidad.

Por último, como tercer punto, desde el punto de vista del usuario, la gestión más débil es la gestión de claves. Todos ponemos más o menos las mismas claves para todo. Porque somos humanos, porque no tenemos memoria. Utilizamos cinco dígitos, que es el nombre de nuestro perro, las iniciales de donde vivo, etc. Totalmente predecibles en un porcentaje altísimo. Además, ahora tenemos una herramienta que antes no teníamos, que es el teléfono móvil, por lo que contamos con un gestor de claves en que podemos delegar. O sea que disponemos de dos líneas diferenciadas en un mismo dispositivo y, dentro de ese dispositivo, de las tarjetas SIM. Estas tarjetas también tienen la suerte de no haberse abierto al mundo exterior, de modo que en esta cadena de valor, donde yo como usuario hasta la aplicación, existen una serie de elementos que me pueden dar un valor añadido, que no necesitan un cambio tecnológico y funcionan en todos los teléfonos, sean *smart* o no sean *smart*. Entonces a nosotros nos sorprende mucho que siendo la realidad como es, solamente algunos (como los bancos o los *googlelianos*) empiecen a utilizar ese nivel de seguridad que son los SMS, ese medio de seguridad que es tremendamente sencillo. Es decir que hay diferentes canales.

Por último, está la SIM. Al fin y al cabo los *smartphones* no dejan de ser ordenadores. ¿Por qué no metemos una firma electrónica (que a lo mejor ya la lleva)? Podríamos garantizar así la seguridad del terminal. Si tenemos la tecnología, usémosla. La reflexión que yo me hago es que quizá la tecnología avanza pero está ahí. Por eso hay que hacer una llamada de atención, no a los usuarios para que se pongan el chaleco antibalas cuando van al centro comercial, hay que hacer una llamada de atención al del centro comercial para que ponga el guardia de seguridad en la puerta. Con la SIM es exactamente igual. Ahí tenemos una oportunidad para hacer las cosas bien.

Por último, voy a hablar del canal. El canal por donde va la información es la cadena de la persona, la aplicación, el dispositivo y dentro del dispositivo el otro dispositivo y finalmente llega a la

persona. Otra de las debilidades está en el canal y en el que los poderes fácticos quieren que esté abierto. Porque si lo ciframos todo, el mundo se queja, porque no se pueden poner controles parentales, no se puede hacer esto, no se puede hacer lo otro. No se quiere que se cifre. Sin embargo, tampoco hace falta ponerle una caja fuerte, podemos ponerle un sobre, y eso tecnológicamente está inventado. La responsabilidad nuevamente no está en el usuario, está en la Administración, en la regulación, en la tecnología y en los poderes en general, a los que les viene muy bien poder mirar cuando lo necesiten. Se puede decir que todos tenemos un cierto interés. En ese sentido, cuando se habla de que geoposicionas, que localizas el dispositivo automáticamente, identificas todo el contexto del usuario. Hay ocasiones en las que para la coherencia en el discurso (llámese operadora o servidor de aplicaciones) es necesario establecer relaciones de confianza, garantizar que la seguridad que no exige demasiadas incorporaciones desde el punto de vista tecnológico funciona, que la regulación acompañe y, a partir de ahí, si somos coherentes, podremos construir muy rápidamente.

El usuario de momento vive feliz. Solo se le remueve la conciencia cuando sale el caso de Snowden, cuando hay un robo de 4 millones de contraseñas. Pero no pasa absolutamente nada, seguimos usando el mismo servicio, la misma contraseña. Yo lo sigo haciendo. Por tanto, fijaos en el nivel de inconsistencia.

Javier Carbonell

Solo quiero hacer un comentario sobre uno de los puntos que has comentado, sobre la utilización del móvil. Esta semana ha tenido lugar el Mobile World Congress y algunos operadores (entre ellos Telefónica) hemos presentado el proyecto de GSMA que utiliza el móvil como método de contraseña. Es lo que se conoce como *Mobile Connect*. Es un proyecto en el que participamos, que acabamos de iniciar, y estamos expectantes ante el posible recorrido que pueda tener.

Manuel Escalante García

Director de Ciberseguridad de Indra

Me gustaría realizar una pregunta a Miguel. Has mencionado el tema de la privacidad, que es un tema que a mí me apasiona. En un mundo conectado, absolutamente global, con regulaciones tan dispares en materia de privacidad, ¿cómo podemos conseguir proteger de verdad la privacidad? Yo estoy contigo, al ciudadano no le preocupa la privacidad. Es más, sabe, consciente o inconscientemente, que haber renunciado a la privacidad le está dando acceso a una serie de servicios en muchos casos gratuitos. Pero lo permitimos.

Por eso, ¿cómo podemos proveer al individuo de privacidad, que él no la va a pelear y que en Europa estamos empeñados en proveer, cuando los grandes servicios *Over The Top* como Google, Facebook, no están en Europa? Seguro que Paloma sabe mucho de esto.



PALOMA LLANEZA

Abogada, socia directora de Razona LegalTech

Preguntas a partir de las cuales se inició su intervención:

- ¿Existe una clara tipificación del delito?
- ¿Qué se está haciendo en materia de legislación?
- ¿Está la Justicia preparada para abordar los conflictos que puedan surgir incluyendo la transnacionalidad?

El sometimiento de las empresas estadounidenses a la normativa de protección de datos está ya contemplado en la normativa comunitaria. El Reglamento Europeo de Protección de Datos establece el sometimiento de las empresas extranjeras a la regulación europea en tanto en cuanto estén tratando datos de ciudadanos europeos. Por ello, si Facebook, Google o cualquier otro tipo de compañía similar quiere operar en Europa tendrá que sujetarse a la normativa europea en cuanto a la protección de datos personales de los usuarios europeos. Además, hemos de añadir que la Decisión de la Comisión de Puerto Seguro fue anulada el pasado 6 de octubre por el Tribunal de Justicia de la Unión Europea, y dejó claro que Estados Unidos no ofrece un nivel de protección similar al europeo, entre otras cuestiones porque hay un acceso sin orden judicial a las bases de datos de todas las grandes corporaciones y porque no existe ningún remedio que te permita ir a un tribunal americano a reclamar tus derechos, a diferencia de los ciudadanos americanos, que sí pueden acudir a los tribunales europeos. De manera reciente se ha aprobado el *EU-U.S. Privacy Shield* (http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm), que establece un nuevo acuerdo transnacional que incluye una serie de modificaciones legislativas en Estados Unidos para permitir a los ciudadanos europeos reclamar sus derechos allí. A tal efecto, el presidente Obama ha firmado la modificación de la *Judicial Redress Act* para permitir a los ciudadanos europeos el derecho a presentar acciones legales ante los tribunales estadounidenses (<https://www.gpo.gov/fdsys/pkg/BILLS-114hr1428enr/pdf/BILLS-114hr1428enr.pdf>). El

nuevo reglamento establece sanciones hasta de 20 millones de euros por infracciones de derechos a la intimidad o de datos y otra que puede llegar al 4 % de la facturación mundial de la compañía. Nos estamos acercando a sanciones de derecho de la competencia. Por tanto, aquellas personas que no pongan en el foco de su negocio la privacidad van a tener que provisionar unas cantidades de dinero importantes en materia de riesgo legal. Además, se incorpora una posibilidad que ya existía en la legislación española pero no en otros países, que es la de poder reclamar una indemnización a quien ha vulnerado tu derecho a la protección de datos. Esta indemnización puede ser limitada en España, pero en países como el Reino Unido o Irlanda, donde existe derecho punitivo, puede alcanzar los millones de euros.

El problema de la protección de datos y la seguridad que ello lleva aparejado se está solucionando en el entorno legislativo. En materia de acceso a la información hay una serie de puntos de inflexión. El primero fue el de la sentencia del Tribunal de Justicia de la Unión Europea, que obligó a Google a borrar el pasado de la gente. El segundo punto de no retorno es el basado en las filtraciones de Snowden. Además, el CEO de Apple dijo en la Casa Blanca que no nos podemos permitir como sociedad el no asegurar la privacidad de nuestros usuarios. Así, la tecnología nos va a dar la posibilidad de proteger la privacidad. Además, creo que en el futuro los productos de privacidad van a ser fundamentales para desarrollar los retos actuales que están surgiendo. Yo soy una convencida de que la privacidad y los productos de ciberseguridad serán fundamentales y se comportarán como un *drive* de la transformación digital. De este modo, siento tener que llevar la contraria en este asunto.

Miguel Pérez Subías

Precisamente, y sin ánimo de llevar la contraria a Paloma, es el discurso que no aporta nada al usuario. De nuevo el foco se pone en las compañías, que está bien también y es importante. Pero no dice nada al usuario. No dice nada de que les vayan a poner una sanción de tantos millones. A mí lo que me importa, y en ello estamos trabajando, es tener herramientas en lugar de poner el foco en la compañía. Por eso a mí como regulador y como usuario me gustaría saber qué sabe o qué tiene Google de mí.

Paloma Llana

Realmente eso ya está pasando, la sentencia de 6 de octubre está basada en el caso de un usuario de Facebook austriaco que le preguntó a Facebook qué tenía de él y la compañía le mandó alrededor de seis mil folios sobre lo que tenía.

Miguel Pérez Subías

Pero como tú muy bien has dicho, eso ha sido un usuario, que ha tenido que ir a un tribunal y ha tenido que esperar unos cuantos años para obtener una sentencia y que luego Facebook le mandara los datos.

Paloma Llaneza

Realmente no tuvo que ir a un tribunal, necesitó acudir a la Autoridad Nacional de Datos Irlandesa.

Miguel Pérez Subías

Pero a mí no me gustaría tener que ir a la agencia irlandesa. A mí me gustaría que me dijera qué sabe usted de mí, que me dé toda esa información y quédese usted si quiere con una copia. Pero déjeme recuperarlo. Por último, ¿y si el dueño fuera realmente yo y el permiso lo tuviera que dar yo?

Paloma Llaneza

Eso ya ocurre, existe una sentencia del Tribunal Constitucional Español por la que se establece que el control sobre los datos es del titular de los mismos y te tiene que dar permiso. Otra cuestión será discutir cómo se redactan esas cláusulas. Pero los datos puedes perseguirlos allí donde estén. El usuario austriaco que ha conseguido con su tenacidad derogar la Decisión de Puerto Seguro se dirigió a Facebook, consiguió sus datos, pidió amparo al regulador irlandés, no se lo dio, y al final lo obtuvo del Tribunal de Justicia de la Unión Europea, consiguió sus datos, etc. Es cierto, y estoy de acuerdo contigo en que en muchas ocasiones no se hace por desconocimiento. Además, mantenemos al usuario en la oscuridad entre los abogados y los técnicos. Pero también es cierto que existen herramientas para ello y no se utilizan.

Almudena Bermejo

Directora de Acción Cultural de Fundación Telefónica

Entonces, mi pregunta después de lo dicho hasta ahora es: ¿por qué mantenemos al usuario en la ignorancia?

Paloma Llaneza

Realmente es despotismo ilustrado: todo para el usuario sin el usuario. Porque les damos un montón de cosas chulas, molonas, televisiones inteligentes, muñecas inteligentes que responden a nuestros hijos y almacenan los datos en una nube. Por eso los tenemos entretenidos en una sociedad infantilizada y les damos unas condiciones generales ilegibles, de cincuenta páginas, que no se pueden leer en la pantalla de un móvil y a lo que los abogados contribuimos cínicamente porque nos pagan por ello. Porque todo se puede hacer legalmente y, si se hace bien desde el principio, cumple con la legalidad. Tenemos una sociedad entretenida con la pantalla, que funciona perfectamente para el que se queda con los datos. Da un montón de servicios al usuario a cambio de datos.

Carlos Abad Aramburu

Director de Soluciones de Seguridad Ikusi

Me gustaría apuntar una reflexión sobre el tema. De todo lo que se ha dicho hasta ahora, me ha dado la sensación de entender que se extrae del usuario toda la responsabilidad sobre la ciberseguridad y se ha delegado sobre la Administración o las empresas de tecnología.

De esta manera, desde un punto de vista filosófico, se hablaba de que al usuario la seguridad no le importa. Con esto yo no estoy de acuerdo. Creo que hay una falsa sensación de seguridad. Si nos fijamos en la pirámide de Maslow, la seguridad ocupa el segundo escalón. Por este motivo, para que funcione cualquier tipo de sociedad o cualquier tipo de modelo, la seguridad tiene que ser un estándar que facilite la generación de cualquier modelo económico. Necesitamos salir a la calle y saber que no nos van a robar. Como sociedad estamos en un proceso de aprendizaje continuo. ¿En cuánto tiempo se han desarrollado las TIC? Y, ¿cuánto tiempo tardamos en terminar una carrera? La sociedad no está preparada ahora mismo para entender todo este tipo de riesgos, impactos, y ese es uno de los principales problemas.

En el informe se presentaban un par de gráficas que a mí me han sorprendido. En ellas se preguntaba si la gente estaba dispuesta a ceder sus datos a cambio de una mejora en las ofertas que le daban. Pues en estos gráficos, la flexibilidad para cederlos aumentaba cuando se les ofrecían mejoras en los servicios, pero disminuía si se les ofrecía una cantidad monetaria. Es decir, la sociedad tiene cierta sensación de que vender los datos está mal, pero si los cedo para obtener un beneficio, está bien. Ahí hay un error de concepto.

También coincido completamente con aquello de que o estás en las redes o no estás. A mí personalmente me pasó que de mis amigos fui el último en hacerme un perfil de Facebook. Al no estar presente, no me enteraba de nada, con lo que me vi obligado en cierta manera. De modo que tienes que estar. Con esto se está generando un modelo de convivencia con la tecnología y no estamos del todo preparados para ello. Además, te generan un incentivo adicional que te hace creer que los servicios son gratuitos. Pero no lo son. Entonces, ¿dónde está realmente el modelo de negocio?

Aquí la responsabilidad, desde mi punto de vista, no es solo de la Administración y de las empresas (que precisamente vivimos de eso). Es una responsabilidad compartida de la sociedad, donde hay que darle a esta los medios para que sea consciente de en qué terreno está jugando. También hay que facilitarles todas las herramientas legales. El asunto de las sanciones es muy importante. Recuerdo que cuando me tocó estudiar el tema de la normativa era cuando se estaba generando el esquema de sanciones que rondaban los 600.000 €. Reflexionando te das cuenta de que existen sanciones, pero al mismo tiempo te das cuenta de que se aplican en casos muy específicos. Como la persona que le solicita a Facebook la información que tiene sobre él y recibe cientos de páginas. Pero ¿cuántas personas hay en el mundo generando esos datos? ¿Y si no somos capaces de acordarnos de lo que hicimos la

semana pasada, vamos a ser capaces de acordarnos de lo que hicimos hace tres años en Facebook? Miré el histórico de mi correo de Gmail y es impresionante la cantidad de cosas que tengo almacenadas. Lo que llaman la huella digital. En referencia a la privacidad, creo que es una cuestión de educación. ¿Yo soy consciente del riesgo que estoy asumiendo al publicar cierta información personal? ¿Cuál es el modelo para que estos riesgos se transfieran y se pueda saber el impacto real?

Paloma Llana

Yo estoy de acuerdo contigo parcialmente en que es extremadamente complicado para el usuario. Pero poner todo el peso en el usuario, cuando estamos hablando de algo tan extraordinariamente complejo técnicamente que solo los que os dedicáis a esto sabéis cómo funciona, me parece excesivo. Por eso, como es técnicamente muy complejo, no es lo mismo explicar a tu hijo que no hay que cruzar la calle cuando el semáforo está en rojo, que explicarle a un niño cómo funciona un teléfono y cuáles son sus riesgos. La complejidad es mayor. Se puede exigir más responsabilidad al usuario cuando exista más transparencia. Este es el binomio, sin transparencia por parte del prestador no se puede exigir al usuario que sea responsable.

Antonio Guzmán

Director de Innovación de ElevenPaths

Me gustaría hacer un comentario. Este debate se está desarrollando en términos de privacidad, regulación, etc., pero yo no sé si tenemos claro cuál es la definición de ciberseguridad. La seguridad nos está protegiendo frente al ciberdelincuente. Tenemos que darnos cuenta de que hay una evolución de esos delincuentes independientemente de que tengamos un marco regulatorio que garantice la privacidad de nuestra información, independientemente de que las empresas tengan que funcionar. Estaríamos hablando de una diferencia similar a la que se da entre los términos ingleses *safety* y *security*. Cuando hablamos de seguridad, estamos hablando de implantar medidas que nos protejan frente a los delincuentes. Podemos tener todo el marco legal que queramos, pero cuando planteamos una evaluación de ciberseguridad, es implantar medidas, mecanismos, políticas que van a levantar una barrera que nos protege frente a la amenaza. Esto no se trata de cruzar la calle. Esto quiere decir que van a existir unos pasos de cebra y voy a tener una regulación. Lo que estamos diciendo cuando se habla de ciberseguridad es que puedo salir a la calle y puede haber un delincuente que me robe. Esta es la diferencia.

Paloma Llana

Lo entiendo perfectamente. Nos hemos ido por el lado de los datos. Lo que ocurre con la seguridad a la que te refieres no hace referencia a la relación contractual que yo tenga con Google. Google se podrá estar llevando más o menos datos míos; mi relación contractual

podrá ser más o menos clara, estará mejor o peor regulada, será más o menos transparente, pero yo esperaré de Google que tome las medidas necesarias para evitar que le roben mis datos.

Antonio Guzmán

En realidad, cuando hablamos de la necesidad de habilitar medidas de ciberseguridad, lo que tenemos que tener en cuenta es que la responsabilidad no es tanto de que nuestros datos estén seguros. Eso es obvio. Sino cómo repercute, qué medidas tienen que habilitar los contenedores, los que mantienen esos datos míos y que yo he cedido. Para que, al margen de que yo haya decidido cedérselos, no acaben en manos de delincuentes.

Este es el problema que trata de resolver la ciberseguridad. Cuando hablaba de la diferencia entre *safety* y *security*, en un entorno industrial es muy sencillo de ver. El *safety* lo que pretende es regular el correcto funcionamiento de acuerdo a un diseño. Tienes que habilitar todos los mecanismos necesarios para que lo que tú has diseñado funcione como tú quieres que funcione. Cuando hablamos de *security*, tenemos que diseñar sistemas para que sean robustos frente a amenazas externas. Esta es la diferenciación que tenemos que hacer.

Por eso es cierto que hay un debate en términos de privacidad, de regulación, legislación, en cómo yo, como usuario, tengo que ser consciente, cómo tiene que haber transparencia. Es una discusión que podemos mantener, pero si queremos tener una discusión en términos de seguridad, lo que hay que hacer es incluir en esa ecuación al atacante y a la amenaza que supone una serie de personas que quieren lucrarse a través de nuestra información, de nuestros servicios o directamente forzándonos a ser víctimas de un fraude.



ELENA GARCÍA DÍEZ

Responsable de Contenidos e Investigación de INCIBE

Preguntas a partir de las cuales se inició su intervención:

- ¿Qué amenazas se están detectando?
- ¿Disponemos de suficientes mecanismos de protección? ¿Qué hace falta?
- ¿Qué consecuencias económico-financieras tienen los problemas de ciberseguridad?

Añadiría aquí que centrar la discusión en los datos, como bien apuntaba desde el principio Miguel, reduce el análisis solamente a una pequeña parcela y no supone para nada el problema global.

A lo que sí nos enfrentamos, en la línea de lo que comenta Antonio, es al hecho de que nos estamos protegiendo de posibles amenazas de «los malos». Malos que están viniendo no solo a por los datos, sino directamente a por los servicios y a por las tecnologías a todos los niveles.

En la actual sociedad de la información tenemos datos y servicios expuestos, lo que supone que nuestras empresas y nuestras industrias están expuestas, en diferentes niveles, a determinadas amenazas que pueden fructificar en un determinado momento o no.

Creo que es necesario abrir la discusión a este ámbito. Porque desde el momento en que abrimos la discusión a servicios y tecnologías, no estamos hablando solo de marco regulatorio y su necesidad, o de nuevas tecnologías muy concretas orientadas al servicio y a la protección del canal, hablamos de toda la infraestructura de los países, de la sociedad en general, que estaba acostumbrada y sabía cómo proteger su infraestructura física. Ahora la sociedad y su economía se mueven en esa infraestructura lógica donde hay que dar respuesta y protección a todos los niveles.

Igual que el usuario está preocupado por sus datos en mayor o menor medida, como hemos estado discutiendo, la empresa y la industria se están encontrando con que su negocio y su prestación de servicio se pueden ver comprometidos en un determinado momento. Por eso, creo que es interesante abrir el debate también hacia ese punto de vista.

Antonio Castillo

De hecho, Elena, las preguntas que te proponíamos eran para que tú incidieras en los temas de las amenazas en general. No solo respecto de los datos de los usuarios. También queríamos saber qué consecuencias económicas y financieras tiene esa falta de seguridad o de ciberseguridad.

Elena García Díez

Efectivamente, las amenazas o la corrupción de la privacidad no dejan de ser una cuestión que está totalmente identificada, si no por el ciudadano o por el consumidor, sí a otros niveles. Por este motivo se promueven regulaciones que vienen a resolver conflictos anteriores que, como bien ha dicho Paloma, se habían detectado. Además, nuestra visión es que los diferentes ámbitos van viendo que la amenaza evoluciona para comprometer su activo o su negocio, su información de mayor interés. Todos los públicos y todas las empresas van identificando que el hecho de tener un virus es un tema de seguridad, puesto que toda la información que tienen en su dispositivo puede quedar comprometida.

Por eso, la evolución de los *ransomware* es patente en todos los ámbitos. El cambio de paradigma que supone decir: «¿Qué ha pasado con mis datos que estaban aquí y yo ya no puedo acceder a ellos? ¿Cómo soluciono esto? ¿Tengo que pagar, pasar por el aro de ese secuestro de datos? ¿Cómo he llegado a esta situación y cómo puedo salir de ella?».

Miguel Pérez Subías

Fíjate, continuamente estamos en una contradicción. Porque ¿cómo le decimos a ese ciudadano o a esa empresa que sea coherente, que tenga un antivirus en sus dispositivos, cuando son los propios cuerpos de seguridad los que diseñan virus para entrar en su teléfono? ¿Cómo les decimos a los ciudadanos y a las empresas que sean coherentes cuando tienen un sistema, como hemos visto en el caso de Apple, y llega el Gobierno y les dice: «Oiga, deme una llavecita para poder entrar en el GSM o en el fax»? Si fuéramos coherentes, cambiaríamos la terminología. Porque queremos hacer lo uno y lo contrario. Esa incoherencia hay veces que anula nuestro discurso. Ya hablo en general, porque al final ya no nos fiamos. Es un problema de confianza.

Antonio Guzmán

Hasta cierto punto no es algo nuevo. Nosotros en nuestras casas tenemos puertas con un cerrojo y con una llave. Y no sé cuántos de los que estamos aquí a lo mejor esa llave la tiene

el portero por si acaso pasa algo. No digo que esté bien o esté mal. Me estoy refiriendo a que es necesario trasladar esa necesidad de protección que todos vemos perfectamente normal en nuestro día a día y en nuestra vida normal al ámbito digital. Porque es algo parecido. Yo ahí voy a tener una presencia, una identidad digital, voy a estar consumiendo, tengo una serie de datos, una existencia en ese ámbito digital, y parece que no es necesario o que no debería ser necesario mantener algún tipo de protección.

Desde mi punto de vista, es prácticamente lo mismo. De la misma manera que yo cuando entro en mi casa, o me voy de mi casa, echo la llave, y es probable que por cuestiones de seguridad, de usabilidad, esa llave la tenga alguien, no significa que no sea necesario mantener este tipo de control. Desde una presencia digital, deberíamos trasladar esa conciencia de esas necesidades de seguridad que tenemos en una vida real a una vida digital.

Ángel León Alcalde

Vocal asesor de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

Efectivamente, hay que trasladar eso. Pero estamos en un proceso que es nuevo para todos. Lo que hay que hacer es preguntarnos cómo se debe trasladar. Tenemos que definir nuevos protocolos. Un protocolo es un modo de resolver de manera estandarizada un problema complejo. No estoy hablando de un protocolo técnico, estoy hablando de protocolos de convivencia o de vivencias de este tipo de cuestiones. Hay infinidad de cosas que históricamente estamos afrontando y seguramente sean mucho más complejas que esto. Por ejemplo, el Derecho, ¿hay algo más complejo que el Derecho? Y, sin embargo, vivimos con ello con cierta confianza. ¿Y por qué? Pues porque tenemos ciertos protocolos, porque hay cierta confianza. Todos hemos firmado un contrato laboral. Pero ¿qué hay detrás de un contrato laboral? Nadie de nosotros lo sabemos, es absolutamente complejo, lo que nos comprometemos con la sociedad, lo que se comprometen con nosotros. Pero es que confiamos porque sabemos que eso forma parte del protocolo. Porque sabes que si tú o la otra parte incumple, te defenderán. Además, por esos mismos protocolos, sabes que estadísticamente hay pocas probabilidades de que vaya a ir mal, y si va mal, se va a resolver razonablemente.

Por todo ello, tenemos que definir un protocolo que permita transmitir esas pautas de seguridad a los ciudadanos y a las empresas en relación con esos temas. Y es lo que todavía no sabemos. Estamos en las cuestiones tecnológicas, en cómo las evitamos, cómo protegemos los datos. Estamos en los asuntos legales, cómo garantizamos la privacidad. Pero ¿y la filosofía para afrontar esta nueva faceta de complejidad de la sociedad? Es un nuevo ingrediente que tenemos que añadir a esta situación compleja que estamos elaborando, y es lo que realmente tendríamos que ir buscando. Pero como ya he dicho, no creo que sea mucho más complejo que el Derecho.

Paloma Llaneza

En realidad el Derecho se basa en la filosofía. Cualquier evolución en este entorno debería estar basada en una reflexión de lo que la gente se quiere dar a sí misma en este ámbito, cómo se quiere organizar, regular, como sociedad. Es fundamentalmente el concepto.

En otro orden, me hace mucha gracia cuando hacemos comparativas entre el mundo teóricamente físico y el mundo digital (aunque siga siendo igual de físico). Me llama la atención que pongáis estos ejemplos como la puerta cuya llave dejo al portero, porque casi nunca me valen estos ejemplos entre el mundo físico y el mundo digital. Os digo por qué y voy a intentar desmontar lo que nos acabas de comentar.

En el mundo físico yo dejo las llaves al portero, que es un señor que conozco, tengo sus datos y al que puedo poner una denuncia en la policía al día siguiente si me ha abierto la puerta. Lo que no hago es dejar las llaves en la sede de la Policía más cercana o en la sede del Ministerio del Interior y decirle: «Aquí tiene la llave de mi casa, entre usted cuando le dé la gana». De hecho, ni al propio Ministerio del Interior se le ocurre, ni lo hace nadie. Es más, para que pueda hacer eso, hace falta una orden judicial debidamente fundamentada o diciendo que se está cometiendo un delito en proceso, etc. Sin embargo, la nueva Ley de Enjuiciamiento Criminal ahora permite los troyanos digitales en las primeras 24 horas sin orden judicial. Así, estas comparativas entre un mundo y otro no son válidas. Porque si le dijéramos a la gente que lo que hemos aprobado en el Parlamento es dejar las llaves de nuestras casas en el Ministerio del Interior, nos pegaríamos al techo.

Antonio Guzmán

Tal vez la analogía que he explicado no se ha entendido. Yo no he dicho que se tenga que dar tu *password* al Ministerio del Interior. Me refiero a que hay mecanismos de autenticación que me permitirían eso.

Paloma Llaneza

Iba al segundo paso. Te voy a comentar por qué eso tampoco me vale. El segundo paso es que existe un problema legal. Hay un problema legal que si no lo resolvemos, con el Internet de las cosas vamos a tener un problema mayor.

Existe una seguridad denominada seguridad de producto. Si yo hago un extintor, tengo que estar sujeto a una normativa de Industria, publicada en el BOE, con una serie de normativa de AENOR para evitar que estalle, conseguir que funcione en caso de que se necesite, etc. No obstante, el *software* es el único producto que se vende sin garantía de que funcione, ni de funcionamiento, ni de que cumpla tan siquiera la funcionalidad para la que lo he comprado.

En el mundo tecnológico nos vamos a encontrar con cosas como el coche autoconducido. Según la última resolución que ha dictado la Administración de Transportes Americana, en el coche de Google no hace falta conductor porque el conductor es el *software*. Como abogados va a ser fascinante porque quiere decir que, a partir de ahora, la responsabilidad va a ser del fabricante del *software* o del responsable de desarrollar el dispositivo de seguridad de ese coche.

Ángel León Alcalde

Respecto a lo que comentas acerca de que el *software* se vende tal cual, tenemos en otros ámbitos de la reglamentación el protocolo consistente en establecer requisitos esenciales que son exigibles para la puesta en el mercado de determinados productos. Se pueden establecer requisitos esenciales para cualquier producto, incluso para un producto *software*. Aún no hemos introducido requisitos esenciales en materia de ciberseguridad. Pero la vía está, el mecanismo técnico e incluso el apoyo legal para hacerlo están ahí.

Paloma Llana

Tendremos que hacerlo. Es una sugerencia que pongo encima de la mesa. Porque tenemos un problema. Porque si ahora vamos a confiar la conducción de un coche a un *software*, este tiene que ser seguro. No puede ser *hackeable* y ha de diseñarse su seguridad desde el inicio. Como abogado lamentaré los tortazos que se puedan meter los coches. Pero vamos a vivir un período muy apasionante donde vamos a tener que ver si la culpa fue de los que fabricaron los sensores, si del fabricante del *software*, el de las actualizaciones, el del coche... Lo que está claro es que nunca más va a tener la culpa el conductor humano.

Antonio Guzmán

¿Y en qué sentido desmonta todo esto que nos has comentado el ejemplo?

Paloma Llana

En el sentido de que si yo compro una puerta, hay una garantía de dos años, tiene que responder sobre la seguridad de la puerta en unas determinadas condiciones que yo he contratado. En el *software*, no; si me lo *hackean*, no tienen ninguna responsabilidad, al igual que si me han hecho un *software* deficiente.

Miguel Pérez Subías

Me vais a permitir que sea un poco irreverente. Fijaos en el debate. Rápidamente, y sigo con la puerta y la llave, hemos hablado de los problemas legales, etc., pero nadie se ha parado a pensar por qué le dejo la llave al portero. Si no hubieses tenido alguna vez el problema de

llegar y no poder entrar en tu casa porque te la has olvidado o una cuestión así, no se haría. El problema no es dejarle la llave a alguien, que yo seguramente no se la dejaría a nadie. El problema es que nos afanamos en que hay un problema del que nadie se pregunta cuál es la causa.

Antonio Castillo

Avancemos un poco más. Porque me ha gustado mucho la intervención de Ángel sobre crear un protocolo. Mi suegro era abogado y me contaba una anécdota de uno de sus primeros casos. Fue un caso de jurisdicción militar, sobre un desertor. Pues bien, le empezó a leer todo el articulado al respecto, hasta que el cliente le dijo: «A ver, para un momento, a mí cuéntame solo los artículos que me favorezcan». Por eso, Paloma, ¿qué artículos nos favorecen?

Paloma Llana

Pues hablemos solo de presuntos «malos». Tenemos varios problemas, por no decir un montón de problemas. Sobre todo en el caso de la delincuencia tecnológica, que es la que más tiene que ver con el debate que estamos manteniendo. Uno de los problemas es en cuanto a la tipología de los delitos penales. Supongo que ya lo sabréis, pero los delitos no se pueden interpretar por analogía. En el terreno civil, por ejemplo, si yo tengo un contrato, puede haber una interpretación analógica sobre cuál es la voluntad de lo que se quiso decir en caso de duda. Sin embargo, en el ámbito penal, lo que está estrictamente escrito es lo que se aplica, no se puede interpretar con algo a lo que se le parezca. Por eso, en España, donde no tenemos un delito de usurpación de personalidad, a diferencia de en Estados Unidos, donde sí lo hay, no nos lo podemos inventar a partir del de usurpación de estado civil o funciones, que sí existe. Por ejemplo, si yo me hago pasar por un teniente coronel de la Armada, pues resulta que sí hay un delito; pero si yo me hago pasar por una persona en Internet, podrá haber un delito por *hackeo*, pero no un delito por suplantación de sus perfiles. No hay delito por usurpación de personalidad en España porque no está tipificado.

Otro problema es que tenemos un legislador que vive atemorizado por Internet y por lo que es el mundo *ciber*. Legisla por impulso, lo que también es muy complicado. Recientemente nos lo hemos podido permitir, porque el Código Penal es una Ley Orgánica y requiere una mayoría cualificada para reformarla. No es algo que se pueda modificar sencillamente, pero que se ha hecho con frecuencia aprovechando la mayoría parlamentaria, en general, a golpe de miedo. Si tuviéramos que cambiar el Código Penal al ritmo al que evoluciona la tecnología, sería complicado.

Esto produce que tengamos unos tipos penales muy estrictos y muy concretos. Antes el *hacking*, es decir, el acceso no consentido en un sistema ajeno y sin autorización, solo era delito como daño informático. Si accedías y rompías algo o dañabas algo, era delito; si te llevabas algo sin daños o simplemente cotilleabas sin dañar, no. Hasta una modificación muy

reciente no se ha conseguido que dentro del tipo de revelación de secretos exista la posibilidad del delito de acceso a un sistema de forma no consentida. Es un delito con una pena de entre seis meses y dos años, que es poco. Porque en este país, con una pena con dos años de cárcel, de manera general, es difícil entrar en prisión si no se tienen antecedentes penales. De manera que esos accesos salen prácticamente gratis aunque accedas a un «pedazo» de sistema. Porque no estoy hablando del delito de estragos, como sería el acceso a unas infraestructuras críticas, que sería un delito diferente, como el acceso a una central nuclear o tumbar toda la electricidad de una ciudad. Eso sería un delito aparte. Estoy hablando de ataques que todos los días se producen a las empresas españolas y que las empresas no cuentan. Donde entran y muchas veces ni las empresas saben lo que se han llevado. Así, sigue siendo una penalidad muy baja en relación con los daños que pueden ocasionar.

La tenencia, distribución, es decir que alguien tenga cualquier *craker* en un ordenador pequeño, puede llevar aparejada la misma pena. Esto también ocurría con el tráfico de estupefacientes, por el que un señor que llevaba 750 gramos en el aeropuerto de Barajas tenía la misma pena de doce años que uno que transportaba 200 toneladas en un carguero. Puede suceder que alguien se descargue un *craker* porque se le han olvidado las claves de su ordenador (y aquí estoy haciendo una presunción a su favor) y le puedan caer los mismos años que a una persona que ha accedido a un sistema de un banco. Esto en cuanto al tipo penal español.

Por otro lado, tendríamos la evolución de las estafas informáticas. El uso de tarjetas de crédito o de numeración de tarjetas de crédito es una novedad y está también dentro del delito de estafa. Ya no requiere el engaño suficiente. Simplemente se necesita el mero traspaso patrimonial con el uso de la tarjeta para ser considerado delito. En cuanto a la famosa figura del *phishing*, que también se ha incorporado al Código Penal, son delitos con una pena máxima de tres años para quien fabrica, distribuye, facilita o posee programas que estén destinados a estafar. De modo que tienen una penalidad muy baja. Los delitos patrimoniales en este país en este tipo de casos salen muy baratos. Resulta más caro que salgamos hoy por la puerta y nos peguen un tirón del bolso porque les pueden caer seis años. Pero con esta tipificación, no le sale muy caro a una persona que se lleve 200 millones de euros de una entidad. Estamos un poco huérfanos desde un punto de vista regulatorio.

Otro problema añadido es el de la investigación, ¿cómo investigo este tipo de delitos? Porque hay una presunción de inocencia y es una presunción muy fuerte. En Penal tú tienes a una persona que es inocente y tienes que traer una prueba de cargo para demostrar que no lo es. Eso requiere una prueba consistente que destruya la presunción de inocencia. La relación causal en el mundo electrónico es muy difícil de establecer. Porque tenemos una IP, un terminal, pero detrás tiene que haber una persona y tenemos que hacer el salto entre ellos y la persona. Es complicado también conseguir este tipo de condenas. Aparte de que los jueces van aprendiendo. Antes se conseguían condenas con pantallazos de WhatsApp. A los abogados que entendíamos un poco de esto se nos abrían las carnes. Esto ha sido así hasta que el

presidente de la Sala Segunda del Tribunal Supremo decidió que no se pueden aportar este tipo de pruebas sin una pericial.

Investigar es complicado, por eso hemos hecho una Ley de Enjuiciamiento Criminal que permite unas entradas por la puerta de atrás de los ciudadanos que no se dan en ningún país de Europa salvo en Alemania, que tiene una figura muy parecida a la nuestra. Y todo esto, solo para pillar a delincuentes españoles. Porque tenemos la siguiente derivada, la delincuencia internacional. La mayoría de los ataques se producen desde fuera de España. Es lo que llamo «los paraísos fiscales de la ciberdelincuencia», donde gente que bien por connivencia con las autoridades locales o bien por ausencia de control hacen de la ciberdelincuencia su negocio. Resulta que para poder solicitar la extradición de un ciberdelincuente fuera del territorio español tiene que haber un tipo penal en dicho país exactamente igual al nuestro. Si no existe, es complicado obtenerla. Para solucionar eso se realizó el famoso Convenio de Budapest, donde se establecen unos tipos penales que tenemos que incluir cada uno en nuestros códigos penales. Pero es de 2001 y está más que superado. Aparte de que lo hemos firmado, hemos incorporado muy pocos de los delitos penales que aparecen en el Convenio de Budapest. Ahí hay un problema. Aunque consigamos identificar al delincuente, tendremos la prueba aquí; a un ciberdelincuente identificado en otro país no lo podremos extraditar con un sistema legal diferente y con una complejidad de la persecución del delito importante. Eso es lo que está pasando ahora.

Lo que estamos viendo ante este estado de cosas y con este tipo de regulación es que hay empresas que se están tomando la justicia por su mano. No daré nombres, pero en la mente de todos está la empresa que *hackea* al que los *hackea*. Por ello, estamos en un territorio sin control porque el Derecho no llega.

Deberíamos comenzar a bloquear la conectividad con ciertos países que son complacientes con el delito. Porque mientras se siga produciendo esa situación, será muy difícil perseguir el delito. En la persecución de estos delitos, el Derecho no está acompañando, y para cambiarlo se necesita de convenios internacionales y la colaboración de los países que no están queriendo hacerlo. Solo queda la autoprotección, que es un poco el Salvaje Oeste donde cada uno tiene que tener su propio rifle.

Antonio Castillo

Creo que el escenario va estando más claro. Hemos abordado al usuario y vemos que está preocupado pero dentro de un orden. Por eso, ahora es el momento de ver qué pasa en la industria. Vamos a empezar por Manuel.



MANUEL ESCALANTE GARCÍA

Director de Ciberseguridad de Indra

Preguntas a partir de las cuales se inició su intervención:

- ¿Qué les están solicitando los clientes industriales e institucionales?
- ¿Los clientes son conscientes de que están amenazados? ¿En qué medida?
- ¿Cuáles son las principales barreras para su implantación?
- ¿Qué implicación tiene la ciberseguridad en el desarrollo de nuevos servicios?

Voy a tener que hacer también una pregunta a Paloma. Vemos que la regulación parece que va a resolverlo todo y luego finalmente tampoco lo arregla. Es una pregunta, subrayo. Internet ha obligado a reinventarse a la industria discográfica, por no decir que en un determinado momento la ha llegado a hundir. Ha obligado a reinventarse a la industria del cine, del *software*, está obligando a reinventarse a las *telcos* que están intentando hacer una mirada ahí. ¡Y ha habido regulación siempre! La regulación está ahí y no ha pasado nada. Las industrias se han hundido, se han tenido que reinventar...

Por tanto, cómo crees tú que tiene que evolucionar el mundo del Derecho. Cuando digo el mundo del Derecho me refiero a las leyes (que están pero están sirviendo de muy poco), a la judicatura, la fiscalía para hacer frente a un problema o un reto que es de carácter global y de un volumen inalcanzable. Para que realmente la sociedad cuando tenga un problema de seguridad acuda al mundo del Derecho, porque la realidad hoy es que es en lo último en lo que se piensa. Si una empresa tiene un problema, intenta resolverlo; si un usuario tiene un problema, parece que tiene que encomendarse a los dioses o lo da por perdido. Porque está muy bien que si uno tiene un problema de intimidad, parece que se resuelve con la Ley de Protección de Datos. Pero la Ley de Propiedad Intelectual estaba ahí y no evitó el hundimiento de la industria discográfica. El *software* y las *telcos* están ahí viéndolas venir.

Paloma Llana

Las discográficas están ahí, reinventándose. Todos usamos ahora Spotify, Movistar Plus y nadie se descarga nada pirata ni ilegal. En primer término, la propiedad intelectual tiene una convención internacional que todos los países firmaron. Es sorprendente lo bien que funciona en materia de protección intelectual la legislación. Es bastante estándar, prácticamente no hay diferencia entre la Ley de Propiedad Intelectual en Estados Unidos, España o Francia. Luego otra cosa es que el mercado se te vuelva en contra y lo que tú vendes no te lo quiera comprar nadie. Pero la legislación es muy similar.

El problema que tenemos con la ciberseguridad es que la protección de los ciudadanos es uno de los *cores* de los poderes públicos y es uno de los *cores* de la soberanía nacional. Es muy complicado que tú te sientes a la mesa con otro país y le digas: «Mira, tu Derecho no funciona, encima tienes ahí a unos señores de la guerra de Bosnia que se han reinventado y se están dedicando a tumbar los sistemas de medio mundo». Primero tenemos un problema geopolítico que hay que solucionar. Pero, por otro, tenemos que ir más allá de la legislación (y esto va en contra del Derecho Penal). Soy muy partidaria de reinventar el Derecho Penal, pero sería muy útil partir del *softlaw* o el derecho más blando. Que establezcamos unos principios muy claros, que tengamos muy buenos principios, muy buenas bases, pero que nos permita una cierta flexibilidad, adaptarnos a las nuevas necesidades que van surgiendo. Eso sí, todo esto sin perder ninguna garantía de los «presuntos malos». Porque si perdemos las garantías, nos habremos perdido como sociedad.

A partir de ahí, hay que gastar dinero en justicia, en fiscalía, en cuerpos y fuerzas de seguridad del Estado. Lo que se invierte en justicia en este país es de risa. Os invitaría a daros una vuelta por cualquier juzgado. Ahora tenemos el sistema LEXNET, en el que teóricamente los abogados estamos presentando los escritos. Pero está siendo tan difícil, que en Madrid nos están obligando a presentar nuevamente los escritos en papel, porque son incapaces de gestionarlo, de tener un expediente electrónico. Tenemos un modelo de oficina judicial del siglo XIX. No llevamos manguitos porque ya no están de moda, pero el modelo es el mismo. Si no se cambia eso, no se invierte dinero en formación, no va a ser posible cambiarlo. Porque a un juez le es más sencillo ver un robo con fuerza, que te peguen un tirón de un bolso. Eso lo entienden y no necesitan ningún *software* para descodificarlo. Pero que tú le vayas con una estafa informática, no. Le da muchísima pereza. Hay muchos jueces buenos, que lo sacan porque les gusta y entienden de informática. Pero lo general es que se vaya sacando del montón de asuntos el resto de los delitos y los delitos digitales se vayan quedando en él.

Antonio Castillo

Ahora vamos a proseguir con el sector empresarial, del que nos iba a hablar Manuel.

Manuel Escalante García

Las empresas se sienten solas en el mundo y la realidad es que lo están. A la pregunta de qué nos piden los clientes, la respuesta depende mucho de las geografías y de la situación geopolítica de la zona. Depende también muchísimo de los sectores. No tiene nada que ver la amenaza y la sensación de amenaza de Asia-Pacífico, donde sienten el aliento de algunos países muy poderosos en Internet y en materia de ciberseguridad, con Europa. En Europa, a lo mejor nos preocupa mucho el fraude, aunque depende del sector, pero en otros países preocupa más el espionaje. En zonas próximas a conflictos, las preocupaciones son otras. En Israel es diferente a otros países. Varían mucho los distintos países del mundo en comparación con donde nosotros estamos. Te das cuenta de que en unos sitios preocupa mucho la filtración: que alguien se infiltre y filtre información. En países con un sector de banca o muy bancarizados y mucha banca minorista les preocupa mucho el fraude y el fraude al cliente final, porque aquello les supone un coste muy grande en seguros, ya que, al final, suele hacerse cargo la banca.

Por sectores también hay muchas diferencias. Sectores que se han desarrollado mucho y muy rápido consumen mucha seguridad, como es la banca o los seguros. El mundo de las *utilities* va entrando y les ha ocurrido alguna cosa, pero de momento no perciben esa urgencia en general. El *driver* suele ser la regulación. Donde hay riesgos para las personas, para las infraestructuras críticas o riesgos sistémicos, el *driver* de la regulación es muy importante.

En general estamos viendo que la cifra de negocio global de la ciberseguridad está creciendo y lo está haciendo bastante rápido. Eso significa que el nivel de sensibilización está aumentando. Primero, no sé si es porque hay más problemas. Segundo, pueden ser más evidentes. Tercero, la regulación empieza a decirnos que eso hay que comunicarlo. A ver si la Directiva NIS termina de salir, pues nos va a ayudar mucho a todos. En el momento en que haya que dar publicidad a los incidentes, nos va a ayudar mucho a concienciar de que es importante.

La ciberseguridad es cara. Es un aspecto que no estaba en los presupuestos de las compañías. Pero está ahí, requiere de tecnología cara y de un personal muy especializado. Ahora mismo este es un cambio en el paradigma de las empresas y cuesta muchísimo calcular el retorno de la inversión. Hay ámbitos donde sí es muy sencillo, como en la banca y el fraude. Si yo consigo reducir el fraude, puedo ver cuál es el retorno de la inversión. Pero hay otros sectores que entran en el ámbito de «qué pasaría si cae un meteorito». ¿Qué pasa si alguien interviene el sistema de una central nuclear? Pueden pasar muchas cosas, pero ¿y si no? ¿Y todo lo que me tengo que gastar y que tengo que detraer de otros sitios? Esa es una de las causas de que no esté siendo rápido. Aunque sí es cierto que la cifra de negocio está comenzando a crecer.

Estamos percibiendo que comienza a haber una conciencia de lo complejo y lo importante que este asunto. Son múltiples tecnologías, cada vez más de nicho, diferentes, para resolver

problemáticas concretas. La navaja suiza ya no sirve, no funciona, ni existe. La ciberseguridad se ha venido comprando igual durante los últimos ocho años. Pero de los dos últimos años a esta parte han aparecido tecnologías más de nicho. Han comenzado a proliferar otros programas adicionales como el Shadow IT, el Vihoran Device, etc., que difuminan el perímetro de las compañías; el *booking* digital cada vez es más complicado y tenemos que aplicar otro tipo de medidas para proteger con otro tipo de foco. El perímetro ya no nos vale. La identidad digital, los mecanismos de autenticación adaptativa, comienzan a tener una presencia muy importante.

¿Qué nos piden? Pues cada vez nos piden más «resuélveme esto». No saben por dónde empezar. Y la verdad es que está muy bien, porque hacerse la ciberseguridad uno mismo no suele salir bien, salvo en la banca, donde hay mucho poderío económico y lo hacen muy bien. Por ello nos dicen: «Resuélvenoslo, dinos qué tipo de tecnología necesitamos, mira cuáles son las amenazas, cuáles son los vectores de ataque que puedan utilizar y dame un servicio completo desde la tecnología hasta la propia operación del servicio». ¿Por qué? Pues porque además funcionan mucho las tecnologías de escala. Una empresa de un determinado tamaño no puede tener expertos en *malware*, que puedan resolver un problema con una amenaza persistente avanzada, no pueden tener expertos en cada una de las materias. Además, suelen ser recursos profesionales escasos. Si un gran cliente quiere tener un equipo completo de nivel dos y tres, es decir, expertos, está agotando los recursos humanos que hay en el mercado. Todos los que estamos aquí sabemos lo difícil que es encontrar determinados perfiles en el mercado. Cada vez más hay una conciencia de la complejidad y de la necesidad, bien porque se entiende la amenaza o bien porque hay un impulso regulatorio. También, como he dicho, las amenazas y las preocupaciones varían por regiones.

Otro aspecto a tener en cuenta es que igual que yo no extiendo mis propias redes para hablar por el mundo, utilizo al operador de telecomunicaciones porque tiene sus economías de escala, porque tienen red, etc., pues da la sensación de que las empresas de ciberseguridad tienen sus bases de inteligencia, tienen sus economías de escala, su *pool* de expertos, etc., que son los que me pueden ayudar, y en el ámbito de la gran empresa esto es lo que se está utilizando más.

También me has preguntado por las Administraciones, y hemos de decir que las Administraciones están corriendo mucho. Porque han tenido muchos problemas y por eso están corriendo mucho. ¿Qué pasa? Que la época del boom de la ciberseguridad ha coincidido con la época del menos boom económico. Esto ha dado un resultado de cifra de negocio raquítrico. Pero aun así se ha notado un aumento en la cifra de negocio en la ciberseguridad en el mundo. Si viene una época de bonanza, la ciberseguridad va a entrar en la agenda no solo en cuanto a discurso y debate, que ya está y ese trabajo ya lo hemos hecho, sino también en cuanto a los presupuestos; que esté en los presupuestos de las compañías. Es más o menos lo que veo en el mundo. Pero ya digo, hay diferencias muy grandes.

Me habláis de las pymes. En referencia a las pymes, va a empujones. Hay un empujón ahora mismo que es el tema del *ransomware*, que son los tipo *lookers*. Y no es una cuestión de que se esté hablando de ello, es que está generando auténticos problemas especialmente a las pymes, que no están acudiendo a la Justicia; es que están pagando y pagar en muchas ocasiones es perpetuar el problema de por vida.

¿Una pyme está preparada para protegerse? No, no lo está. Una pyme seguramente lo que necesita es poner su seguridad en manos de alguien que haya diseñado ese entorno empresarial con seguridad *by design*.

Paloma Llanea

¿No crees que con una aplicación o con unas buenas prácticas, que no realiza prácticamente ninguna pyme, se podrían solventar una parte importante de los riesgos constantes que tienen? También sé que es cuestión de tiempo que la sofisticación del *malware* lo destruyera. Pero si vas creando unas buenas prácticas, a lo mejor consigues que en algún momento se enganchen y se incorporen.

Elena García Díez

Probablemente ese es el primer paso, pero aquí es clave tener en cuenta la problemática particular de la pyme, que no tiene la madurez de la gran empresa para consumir ciberseguridad. Quizá esa falta de madurez también la acusa la industria de la ciberseguridad en su capacidad de prestación de servicios a la pyme. Ante los grandes sectores sí hay madurez. El sector financiero sabe que tiene que consumir ciberseguridad y hay una industria perfectamente preparada para prestarles los servicios que requieren. En la pyme esto no es así.

Aunque estemos trabajando en la sensibilización y en crear códigos de buenas prácticas, es fundamental trabajar la demanda de la pyme y generar una oferta de servicios convenientemente adaptada. El contexto es complicado, y por eso desde INCIBE estamos trabajando en ello. La llegada del *ransomware* y el gran impacto que está teniendo está dando un impulso fuerte a la concienciación sobre el problema que puede suponer la falta de ciberseguridad ante un ataque.

En otros casos, seguimos asistiendo al clásico «¿A quién le van a importar mis datos?».

Ángel León Alcalde

Y en línea con lo que comentáis de la necesidad de externalizar los servicios de seguridad y más con quien no tiene capacidad como son las pymes, ¿no pensáis que el sector de los seguros o los ciberseguros podría jugar un papel muy importante aquí? Igual que en otro tipo de riesgos. Si soy una pequeña empresa aseguro hasta determinado punto mi riesgo y, ade-

más, la prima que pago depende de las medidas de ciberseguridad que tenga. Por tanto, serían las compañías de seguros las que me ayudarían a mí a protegerme y aminorar el riesgo.

Manuel Escalante García

Precisamente se celebró la semana del seguro y ayer tuvimos una charla en la que hablamos sobre ciberseguridad en el seguro. Por supuesto que sí, Ángel, esto era cuestión de tiempo. Los que nos dedicamos a esto lo estábamos viendo venir. Pero no se trata solo de pymes, también se trata de grandes empresas. Date cuenta de quiénes son los que están «cayendo». Vete a cualquier listado de incidentes graves. No son pymes, son «pedazos» de empresas que invierten muchísimo en seguridad y están teniendo contratiempos muy importantes. Yo ya no puedo invertir más, o probablemente puedo invertir más, pero, ¿dónde invierto lo suficiente para no tener problemas? Como ha dicho Andrés, la sofisticación de la amenaza es creciente y va a seguir siéndolo. Habrá que hacer una transferencia del riesgo hasta donde se pueda transferir, porque se puede transferir solo hasta un punto.

Ángel León Alcalde

Yo no me refería tanto al proceso de transferencia del riesgo, sino cómo ayuda el seguro, más allá de una campaña de concienciación que podamos hacer. La aseguradora cómo ayuda, un colaborador nuestro, que nos aporta experiencia y tenemos un beneficio mutuo.

Carlos Abad Aramburu

Sobre este tema, he estado leyendo recientemente y he identificado cierta tendencia a desarrollar el negocio de los ciberseguros. Lo que ocurre es que para que un ciberseguro sea efectivo, se necesita respaldo jurídico. Precisamente lo que hemos comentado es que el contexto legal actual no lo ofrece. La duda que se repite es cómo materializar un seguro en caso de un ciberataque.

Paloma Llanea

En este ámbito dos apuntes, la Ley de Contrato de Seguro no tiene nada que ver con el ciberriesgo. El problema, efectivamente y como bien dice Carlos, es cómo materializar un seguro en caso de un ciberataque. Seguramente lo que tenemos que hacer es hablar con las compañías de seguros y estandarizar unas condiciones generales de contratación que de momento no lo están. Entre otras cosas porque los clientes te lo piden.

He leído muchas condiciones de contratación de seguros y no te cubren nada. Prácticamente te cubren el pagar una empresa de comunicación para decir: «Tranquilos, no ha pasado nada, sus claves están muy seguras»; un gabinete de crisis, algo de daño a terceros, que en el caso español es muy difícil calcular el daño patrimonial a terceros cuando no sabes si se han utiliza-

do tus claves, si se ha hecho algo con ellas. Porque a lo mejor se están vendiendo en el Internet profundo pero tú no tienes ni idea. La verdad es que el daño propio no te lo cubren nunca. Porque lo que tú necesitas es recuperar un sistema que te han tumbado. No es como una póliza para cubrir un incendio. En el mundo *ciber* comentas: «Me han hecho un roto de tanta cantidad, me tengo que gastar tal dinero en arreglarlo», y te contestan: «No, esto está excluido».

Manuel Escalante García

Yo estoy de acuerdo con Ángel. Estoy también de acuerdo con Paloma en que en el daño propio no vas a conseguir nada. Pero tú ponte en el lado de las pymes que se ponen a vender en Internet. Pueden tener un problema de privacidad por muchas medidas que pongan. Si les está pasando a las grandes, cómo no les va a pasar a las pymes. Solo eso es una gran ayuda. Porque yo siempre me hago la misma pregunta (y del mundo pyme algo conozco): ¿cómo de gruesa tiene que ser la puerta para que si entran (que si alguien lo intenta, lo va a conseguir, por muy gorda que sea la puerta) no me pongan a mí la sanción? Eso por supuesto no te lo va a responder nadie. Pero yo tengo un residual de riesgo que no puedo cubrir y que tengo que transferir. Por eso creo que ante situaciones como estas, el mundo del seguro puede resultar de gran ayuda. Estoy totalmente de acuerdo en que del daño patrimonial no vas a conseguir nada, pero pueden ser de gran ayuda.

Paloma Llana

Hay un elemento final. Las compañías de seguros trabajan con actuarios y series estadísticas que establecen la prima que tienes que pagar por un determinado riesgo. Como hay una total opacidad de información en el mundo *ciber*, los actuarios de seguros no saben cómo calcular las primas. Puede ser que ahora, con la obligación que va a haber de comunicar, van a tener más datos para calcular. Porque un actuario es capaz de saber cuánto cuesta la muerte de una persona de 39 años, casado y con hijos, si eres mujer u hombre, etc. Te sacan las cifras y te hacen el cálculo. Pero en el mundo *ciber* de momento no hay datos para calcular.

Antonio Castillo

Creo que Manuel ha dado una visión muy detallada del mundo industrial. Nos ha explicado la situación de las grandes empresas, luego de las pymes, y sobre todo un panorama de cuál es la demanda actual.

Ahora me gustaría centrarme en Carlos, que proviene del mundo de la seguridad física. Yo creo que de la seguridad física siempre ha habido conciencia. La gente ha sido mucho más consciente de esa problemática. Aunque luego, como se ha comentado, se le deje la llave al portero. Pero, sobre todo, desde el punto de vista de las empresas, ¿cómo veis vosotros ese traslado de la seguridad física hacia la seguridad informática? ¿Cómo lo estáis viviendo en España, donde tenéis un modelo de negocio, y en México, donde vendéis otro?

Luego ya, con José Valiente, nos gustaría insistir en esas prácticas de ciberseguridad desde el principio. Como hemos visto, hay dos posturas, como en casi todo: la concienciación de los usuarios y la tecnología. Creo que es importante enfocar esos dos puntos de vista. El de la prevención, que es muy importante, y el de la tecnología. Seguramente, ambos sean complementarios y se necesiten el uno del otro.



CARLOS ABAD ARAMBURU

Director de Soluciones de Seguridad Ikusi

Preguntas a partir de las cuales se inició su intervención:

- ¿Cómo está evolucionando la demanda clásica de seguridad física al incorporar elementos de seguridad digital? ¿Cómo se complementan?
- ¿Cuál es la importancia de la ciberseguridad en la gestión de instalaciones?

Desde mi punto de vista y desde la actividad que desarrolla Ikusi, contamos con dos modelos de negocio diferentes, si comparamos las soluciones que ofrecemos en seguridad electrónica con la ciberseguridad. En cuanto a la seguridad electrónica, el período de aprendizaje ha sido mucho más largo que en la ciberseguridad. Este factor es clave, porque están involucrados sistemas tecnológicos sin estándares, responsables y mandos, regulaciones y un contexto acotado y específico en cada caso.

Como bien ha dicho Manuel, estamos inmersos en un periodo de tiempo en el que la crisis económica ha afectado a este sector, y uno de los *drivers* fundamentales para mejorar el retorno de la inversión es incorporar tecnología. El problema es que la tecnología se está integrando desde un punto de vista puramente funcional y operativo. No se está teniendo en cuenta la segunda derivada, que es la dependencia de los sistemas de comunicación y la parte de la infraestructura interna. Estamos hablando desde la propia generación del producto o solución específica (aplicaciones, *software*, diseños, integración con arquitecturas existentes). Es este el tipo de problemas que estamos teniendo.

Luego existe otro mercado, el de la parte de integración de redes y comunicaciones. Procede de un mundo donde lo primero era dar la conectividad, garantizar la disponibilidad y luego, como valor añadido, ofrecer un servicio de seguridad. Precisamente se da este último servicio para garantizar principalmente la disponibilidad de las comunicaciones, principales *drivers* de inversión que nos estamos encontrando.

Uno de los retos principales que estamos viendo es cómo le damos coherencia a este contexto. Desde el punto de vista de la parte de seguridad, tenemos una dependencia y hay una convergencia de amenazas. Por un lado, se contempla la seguridad física para proteger activos lógicos. Y por otro, desplegamos una infraestructura TI segura sobre la que se soportan sistemas de videovigilancia, datos de seguridad almacenados como metadatos procedentes de sistemas de análisis de contenido de vídeo o generación de evidencias legales para poder acometer procesos legales. Este es el contexto sobre el que hay que generar una base de seguridad sobre esa información. ¿Qué ocurre cuando unimos esos dos mundos y la amenaza es una amenaza convergente? Tenemos el ejemplo, en 2008, en Georgia, el ataque en Osetia del Sur, en el que se inutilizaron los sistemas de información y posteriormente se llevó a cabo una incursión por parte del ejército ruso.

Un punto a tener en cuenta es cómo están estructuradas las empresas y los órganos de decisión en estos momentos. Las empresas lo están de una forma vertical, como es el caso de la seguridad física, con un amplio conocimiento en mecanismos y procedimientos casi siempre orientados al tiempo real. En este contexto, cuando vendemos tecnología de seguridad electrónica, lo que vendemos es tiempo; se trata de que el operador tenga una capacidad de reacción mayor para utilizar menos recursos y de forma más eficiente, sin perder de vista la efectividad.

Sin embargo, cuando nos trasladamos al mundo de la seguridad de la información o ciberseguridad, se presentan unos modelos y tiempos de trabajo totalmente diferentes. Por ejemplo, como atacantes, podemos desarrollar una amenaza persistente avanzada, tema muy de actualidad, y podemos introducirla a través del propio usuario para que infecte toda la instalación y genere un vector de ataque totalmente diferente. Este hecho nos obliga a desarrollar modelos de gestión totalmente distintos. Cuando vamos a plantear un proyecto de integración, no existe, por norma general, un mecanismo en las organizaciones que te permita trasladar esta preocupación a la vida real de forma efectiva. Es necesario cubrir un *gap*, principalmente de entendimiento. Hay un departamento que habla un idioma y otro en el que se habla otro. Realmente, ¿de dónde vienen las inversiones? Resulta que tenemos proyectos tradicionales, como el sistema de seguridad electrónica, con unos requerimientos muy específicos sobre qué es lo que debe protegerse y, en muchas ocasiones, existe un apartado como el del despliegue de la red de comunicaciones. Eso queda a tenor del integrador y, generalmente, la empresa tradicional de seguridad electrónica no tiene grandes conocimientos en la parte de red. Para nosotros, este asunto es de gran sensibilidad.

Por otro lado, también hay un problema con los modelos de contratación. Generalmente se publican pliegos diferentes cuando se trata de soluciones OT, como la seguridad electrónica o soluciones de comunicaciones, o IT, en que la componente de servicios y/o productos varía con respecto al primer grupo. Nosotros, como empresa, estamos viendo que existe una difi-

cultad a la hora de trabajar este escenario. Sabemos que hay un problema conjunto, que existe una amenaza real. Por ejemplo, ejecutando un ataque de denegación de servicios contra un sistema de videovigilancia, lo que realmente se logra es condenar una infraestructura, que evita la posibilidad de efectuar una respuesta operativa efectiva. Por eso, actualmente nosotros nos estamos planteando cómo generar un modelo de contratación válido que aporte valor a la empresa.

Desde el punto de vista de las empresas tradicionales de desarrollo de producto de seguridad electrónica, observamos que están ahora centradas en productos de alto nivel, principalmente productos *software* y su integración. ¿Qué ocurre con el modelo de ciclo de vida de *software* seguro de McGraw? Establece bien claro que la mayoría de los problemas de seguridad se concentran en las fases de diseño, mantenimiento y operación. Si trasladamos este concepto a los proyectos, generalmente estas partidas son sensibles a reducirse tanto en la contratación como en la ejecución. Es decir, el diseño se realiza atendiendo a las funcionalidades principales y a la arquitectura existente, sin tener en cuenta requisitos de seguridad. En relación con el mantenimiento, no es que sean poco profesionales, sino que están muy orientados a la operación; por ejemplo, que la cámara vea o no dependiendo de si la conexión es segura. Podemos implementar un sistema de seguridad electrónico totalmente competente y con una tecnología buena desde el punto de vista operativo, pero, ni su diseño ni su mantenimiento están siendo adecuados para la propia seguridad del sistema.

En el sector de los fabricantes, ¿qué ocurre con ellos? Ahora mismo el mercado no está dispuesto a pagar una aplicación que contemple mecanismos de ciberseguridad. Supongamos que tenemos dos aplicaciones de centro de control; la primera transmite la información de forma cifrada, tiene un control de acceso e identidad mejor y dispone de mecanismos de control de integridad de la información. Pero claro, estos beneficios conllevan un incremento del coste de un 50 % más. Sin embargo, el cliente actual únicamente quiere un centro de control para integrarlo con los sistemas que tiene y que le permita operarlos y desarrollar sus mecanismos operativos de seguridad física. El mercado no está dispuesto a pagar el sobrecoste de la ciberseguridad en productos de seguridad electrónica. Al mismo tiempo, tampoco existen unos estándares claros e implantados para el desarrollo de aplicaciones seguras que faciliten la comparación de productos al cliente final. Sí encontramos diferentes modelos para implementar seguridad en el *software*, pero para el desarrollador es caro incorporar un departamento que lo desarrolle, mantenga y actualice de forma segura en este sector.

Nosotros hemos observado que existe este problema, que la industria no está preparada para resolverlo y que, actualmente, las organizaciones han iniciado ya un proceso de cambio. Empezamos a tener más interlocución con los responsables de IT, y esto es importante. Pero todavía nos queda una vuelta de tuerca adicional, que es que los procesos de contratación nos permitan, a las empresas que estamos capacitadas para ofrecer estos servicios que con-

templán tanto la parte de operación como de información, poderlo poner en valor. Simplemente necesitamos un reconocimiento por parte del mercado.

Respecto a la diferencia entre los modelos de negocio de Ikusi en materia de seguridad, podemos decir que tenemos uno orientado al proyecto, que es el de la seguridad electrónica, y otro al servicio, que es el de la ciberseguridad, fácilmente externalizables por parte del cliente debido a su incapacidad, en muchas ocasiones, a la hora de incorporar servicios propios por el elevado coste que tienen.

¿Dónde vemos que se está generando un catalizador de esta necesidad en cuanto a la oferta? En las empresas de seguridad privada. Ayer tuve la oportunidad de visitar la Feria Sicur. Las principales empresas de seguridad privada a escala global reforzaban su oferta de tecnología, impulsada por su impacto en la mejora de su rentabilidad. Somos conscientes de que la industria está tendiendo a converger entre la parte de seguridad electrónica y la parte de ciberseguridad. Tiende hacia un modelo puramente de servicios, e incorpora la parte de los servicios activos de vigilancia. Esto de cara a las Administraciones y a la industria ofrece un valor añadido fácilmente identificable. Desde la perspectiva de las empresas tecnológicas del sector, es necesario desarrollar un proceso de asimilación y adaptación. Entonces lo que se está diciendo al mercado es «encaminémonos a una solución integral» porque las aplicaciones *software* específicas de seguridad, los estándares de comunicación y los dispositivos o sensores que se fabrican nos permiten generar un modelo eficiente en recursos y al mismo tiempo efectivo, gracias a una mayor automatización. ¿Todo esto en qué deriva? En que para la industria de la seguridad electrónica, la seguridad de la información es fundamental.

Una de las iniciativas erróneas, que creo que se ha madurado, es el concepto de «único centro de control». En su día pude leer artículos que hablaban del concepto de «centro de seguridad integral», donde había un centro de seguridad físico y lógico operando bajo una misma plataforma tecnológica. Si analizamos las ventanas de tiempo en ambos casos, son totalmente diferentes. En cuanto a los perfiles de los operadores, también son totalmente diferentes, así como los procedimientos de actuación. Esos dos entornos deberían estar separados a nivel de operación, pero contar con un cuadro de mando conjunto. Este es el tercer mecanismo de convergencia. Estamos tratando el concepto de inteligencia, destino hacia el que deberíamos dirigirnos. Ante esta situación, la pregunta que tendríamos que hacernos es: ¿por dónde empezar? ¿En qué sectores? La respuesta debe ser la de comenzar por las infraestructuras críticas, que es donde suponemos que va a haber mayor demanda, si es que no la hay ya.

En el ámbito de las pymes, lo veo difícil y tengo mis dudas, porque al final, detrás del ciberdelincuente, hay un modelo de negocio. ¿Qué gano? ¿Cuál es la inversión que tengo que hacer para generar un beneficio? Si el objetivo es la pyme, parece que está claro que el tipo de ataque más habitual es el *ransomware*. Este modelo ya se conocía, era conocido como «el virus

de la policía», era un *malware* relativamente sencillo de construir, con un factor de escala tremendo, distribución rápida, impacto monetario pequeño con rápidos pagos. Ahí es donde tenemos que aplicar la seguridad en las pymes. No tenemos que aplicar la seguridad de las pymes en las APT (amenazas persistentes avanzadas). Son los mensajes erróneos que se están generando en el mercado. Hablamos de ciberseguridad y la tendencia actual es centrarse en las APT. Pero ¿cuánto cuesta desarrollar una APT? Y sobre todo, uno de los factores fundamentales es que tienen un objetivo único. Son amenazas dirigidas a un determinado sector. Por tanto, en este contexto definido, lo que tenemos que hacer es partir desde la especificidad del sector, identificar las amenazas particulares, definir exactamente cuáles son los niveles de riesgo y de impacto y, con esta información, generar especialistas verticales.

Volviendo a las infraestructuras críticas, sabemos que hay una amenaza real. Existen grupos organizados en un entorno que está desorganizado. A esto tenemos que añadirle la existencia de interdependencia entre los países. En España tenemos un instrumento interesante, la Ley PIC. La Ley PIC genera un estándar, los planes de seguridad del operador, que no es nada más que poner en orden los planes de seguridad tradicionales. Desde el punto de vista de la tecnología, la clave reside en los planes de protección específicos. Ahí es donde realmente se va a ver si está teniendo éxito la norma.

Por último, si nos alejamos del mercado nacional y nos trasladamos, por ejemplo, al mercado latinoamericano, donde la cultura en seguridad, la regulación y el estándar de utilización de tecnologías es diferente, percibimos cierta tendencia de forma nativa a relacionar ambos mundos, el de la seguridad física/electrónica y la ciberseguridad. Este hecho plantea una oportunidad real para el modelo que estamos desarrollando.

Manuel Escalante García

Hay un tema muy interesante ahí que no has mencionado. Lo digo por la diferencia entre el mundo anglosajón y el de Europa. En Europa contamos, por ejemplo, con regulación para el mundo *smart machinery*. Existe la regulación, pero cuando tú vas a implementarla, no hay norma. Por el contrario, en Estados Unidos sí hay norma, pero no hay ley, de modo que sí se está desarrollando su implantación. Pero cuando tú quieres hacer implantaciones de perfiles *smart machinery* en Europa, te tienes que ir a la normativa del NIST (National Institute of Standards and Technology). ¿Lo estamos haciendo bien? Yo me lo plantearía. Es verdad que la referencia en Gateway es alemán. Yo creo que por puro azar. Porque metemos un montón de leyes, pero luego a la hora de la implementación...

Simplemente, un caso que creo que ilustra muy bien el tema de los *drivers*. Las eléctricas invierten relativamente poco en seguridad. Tenían un problema de fraude en las distribuidoras, y es que si alguien ponía un imán encima de un contador, aquello no contaba y había cierto fraude. Pero ¿qué pasa cuando hay una ley que me obliga a tener redes de medida inteligente? Pues que tengo una red de datos que llega hasta los hogares. Si me enchufa en mi

casa y pongo un módem, estoy en la red de datos. No es tan sencillo, estoy simplificando. Tendrás que suplantar el contador y hacer muchas cosas, pero esto ya no es el imancito con el que sí hay fraude. Por eso es el *driver*, es el posible fraude, y no hay ni una sola eléctrica grande en la que no estemos trabajando en la seguridad de *smart machinery*. Y no es debida a un riesgo sistémico. No hay una amenaza clara, porque no la hay. De hecho se han disparado ciertas alarmas que no son ciertas, porque, además, las eléctricas españolas están muy preparadas. Pero es verdad que el canal está ahí para que alguien en un determinado momento consiga encontrar un puerto de depuración abierto y comenzar a trabajar. Esto evoluciona cuando hay algo muy concreto, como el fraude; es rapidísimo. El presupuesto de ciberseguridad de repente es un escalón. Sin embargo, cuando no hay un *driver* económico, va muy despacio, incluso con un impulso regulatorio. Fíjate que el CNPI lo está haciendo bien, pero es muy lento.

Carlos Abad Aramburu

Efectivamente, se está creando un buen contexto, pero es cierto que el mercado de la ciberseguridad funciona por regulación, por miedo (le ha pasado algo a él o bien al vecino) o por conciencia propia. Sin embargo, la conciencia propia solo funciona cuando hay presupuesto.

Miguel Pérez Subías

Habéis dicho que en los lugares donde los *drivers* funcionan es porque hay norma y a lo mejor no regulación. Esa norma ¿quién la crea?, ¿los organismos nacionales, el Ministerio, organizaciones internacionales?

Antonio Castillo

En Estados Unidos, la normativa suele ser de impulso industrial, que además no acostumbra a ser obligatoria. Una norma americana no puede ser obligatoria porque va contra su naturaleza. Se realiza a través de un consorcio industrial que se encarga de ello; a través de la American Standard Society. Es más, incluso te puede pasar (en Europa sería inconcebible) que haya dos normas, como ha ocurrido en el campo de la informática durante mucho tiempo.

Manuel Escalante García

El National Institute for Standards and Technology es el que emite este tipo de normas y es muy potente.

Carlos Abad Aramburu

Hay un tema importante. Hemos puesto el foco, como dice Manuel, en aquellos procesos que son operativos y están relacionados con el desarrollo de la actividad o proceso producti-

vo de la infraestructura. Ahí el *driver* es claro. Sin embargo, hay procesos que son de soporte y no por ello carecen de importancia, como por ejemplo la seguridad. Estos procesos de soporte hacen también uso de sistemas tecnológicos y pueden tener un impacto indirecto en el negocio, con lo que deberíamos preguntarnos: ¿dónde colocas el de la ciberseguridad? ¿Únicamente en los procesos productivos? ¿Qué ocurre con todos los procesos de soporte que se fundamentan en sistemas OT?

Es bastante común escuchar a un cliente afirmar: «Yo ya tengo mi plan de seguridad, mis cámaras, tengo mi control de acceso perfectamente operativo y aquí poco más podemos hacer». No obstante, resulta difícil tener conciencia de que dentro de su proceso productivo la seguridad es un proceso de soporte. Pongamos como ejemplo un aeropuerto, sobre el que podemos definir tres zonas de seguridad: pública, restringida y crítica. En estas infraestructuras existe lo que se conoce como «la línea tierra-aire», que permite separar la zona pública de la crítica. Debido a la normativa existente, es necesario facilitar la evacuación y por ello deben existir puertas de evacuación que permitan atravesar dicha línea. Estas puertas están controladas por sistemas de seguridad electrónica, que en España son responsabilidad del Departamento de Seguridad. En primer lugar, debemos ser conscientes de que existe un proceso operativo de soporte adicional a los procesos de negocio del aeropuerto, como son el movimiento de equipajes, aviones y pasajeros. En segundo lugar, debemos ser conscientes de que este proceso de soporte hace uso de una tecnología que mejora la eficiencia mediante el control automático desatendido de las puertas de evacuación. En el supuesto de que se ejecute un ataque que provoque la apertura no controlada de las puertas, tendría un impacto muy importante tanto en el plano económico como operativo de la infraestructura. En ese caso se tendría que realizar un procedimiento de esterilización, que conlleva un coste muy elevado. En el peor de los casos, habría que desalojar el aeropuerto o las zonas afectadas, para poder revisarlas de forma exhaustiva por parte de las fuerzas y cuerpos de seguridad del Estado. En este caso, la regulación se cumple, pero no se es consciente del riesgo asociado que supone incorporar al proceso la tecnología que depende o es sensible a factores relacionados con la ciberseguridad. Actualmente vemos que el foco está en los procesos operativos directamente relacionados con el negocio, en particular cobran especial importancia los sistemas SCADA.

Estos son los *drivers* que a la industria le preocupan actualmente, y no podemos caer en el error de olvidar los procesos de soporte, que cada vez son más sensibles a la ciberseguridad.

Antonio Castillo

Visto esto, vamos a pasar a la última parte del mundo industrial. Eso sí, luego recuperamos dos asuntos que ya se han tratado aquí, como son las infraestructuras críticas, sobre el que preguntaremos a Ángel, y también otro que está pasando un poco desapercibido, como es el del IoT, sobre el que nos explicará Antonio Guzmán.



JOSÉ VALIENTE

Director del Centro de Ciberseguridad Industrial

Preguntas a partir de las cuales se inició su intervención:

- ¿Qué tendencias tecnológicas están surgiendo en torno a la ciberseguridad industrial?
- ¿Qué sectores industriales se están viendo más afectados por las amenazas de seguridad IT?

En primer lugar quería dar respuesta a las tendencias tecnológicas sobre la ciberseguridad industrial para aquellos que no lo conozcan; igual que hay sistemas de información, que todos conocemos, como el correo electrónico, los ERP en las organizaciones, existen también las tecnologías de operación, para los procesos de operación, aquellos que permiten automatizar esos procesos industriales. Como ha comentado Carlos, los sistemas SCADA, controladores como los PLC...

La mayor parte de las organizaciones industriales tienen muchos procesos automatizados y dependen tecnológicamente de ellos para que la energía se genere, se distribuya, para que se fabrique cualquier tipo de producto, etc. La tendencia tecnológica es que, para protegerlos, primero hay que poner en contexto estos sistemas de operación. En los sistemas de operación tienen mucha fuerza los fabricantes industriales. Los fabricantes industriales que proporcionan la automatización de sus refinerías a un Repsol o a un Cepsa tienen un poder enorme. Tan grande, que no te permiten incluir ningún *software* de protección en sus sistemas porque si lo haces, dejarían de mantenerlos. Por este motivo, las medidas para proteger estos sistemas de operación no pueden ser intrusivos. Normalmente las tecnologías que podemos utilizar aquí para proteger estos entornos provienen de las comunicaciones. Y debe hacerse mediante la observación, mirando, no interceptando nada, porque lógicamente podrías afectar a la producción.

Este es el entorno. Los fabricantes tienen mucho peso y no se pueden poner sistemas de protección *software* en los sistemas SCADA, historiadores, etc. ¿Cuáles son las tendencias en

cuanto a tecnologías aquí? Pues por un lado, hemos observado que cada vez más hay simuladores que nos permiten identificar las amenazas; por ejemplo, en los dispositivos inteligentes; por ejemplo, en los *smart metering*, donde existen herramientas que te permiten colocar en una arquitectura una serie de dispositivos inteligentes, simular una serie de amenazas y obtener las medidas que deberías aplicar. Porque al no poder aplicar las medidas en el entorno de producción, los simuladores son una de las tendencias.

Otra tendencia es que los laboratorios puedan certificar las tecnologías industriales. Un fabricante como General Electric, o como Siemens, tendrían que superar una serie de pruebas por parte de algunos laboratorios para que esa tecnología estuviera certificada y se pudiera implantar. Precisamente, en Europa estamos participando en un foro que se llama ERNCIP (European Reference Network for Critical Infrastructure Protection), donde se está trabajando precisamente en eso, en definir cómo se van a certificar estas tecnologías industriales.

Otra de las tendencias tiene que ver con que, aparte de las comunicaciones, también se utiliza mucho USB en el mundo industrial. Con ello se trata de tener la certeza de que la seguridad del *pendrive* es el autorizado. En esto también se está trabajando. Indra, por ejemplo, tiene algunas herramientas de *sanitización* en este aspecto.

En el ámbito de los fabricantes industriales también se está trabajando y se están incluyendo medidas para poder protegerlo. Sobre todo en cuanto al control de acceso a las aplicaciones. Había comentado que los fabricantes no permitían que se pusiera un *software* ajeno u homologado por ellos. Por eso están empezando a desarrollar sistemas de seguridad. Por ese motivo cada vez estamos viendo más anuncios en la prensa de fabricantes de tecnologías industriales que llegan a acuerdos con un fabricante de ciberseguridad como Palo Alto o Intel Security.

Otro ámbito y tendencia de protección es el de la monitorización de redes *wifi*. En el ámbito industrial cada vez se están utilizando más estas redes, porque resulta carísimo cablear todos los sensores y actuadores. En una refinería puede haber cientos de miles de kilómetros de cables en los que deberían colocarse los sensores necesarios para automatizar los procesos. Se está intentando abaratar todo ese cableado a través de tecnología *wifi*. Por ello la monitorización de las redes *wifi* para identificar problemas de seguridad es otra de las alternativas.

Otra de las preguntas que me hacía Antonio es qué sectores industriales se están viendo más afectados por las amenazas de ciberseguridad. Esto no se puede responder fácilmente. Para contestar a esto tendríamos que tener cierta información, y nadie la tiene. Lo único que podemos cuantificar es el número de incidentes que se han reportado. Estos informes se envían a los CERT. El CERT que más tiempo lleva haciéndolo es el de Estados Unidos, el ICS-CERT, que es un CERT especializado en las notificaciones de eventos sobre sistemas de operación y sistemas de automatización industrial.

Os voy a dar algunos datos para que os hagáis una idea de lo que ha ocurrido en los últimos tres años. En 2013 se comunicaron aproximadamente unos trescientos incidentes sobre sistemas de automatización industrial. De esos trescientos incidentes, casi el 60 % eran incidentes reportados por el sector de la energía (eléctrica y petroquímica); el 16 % de lo que ellos denominan fabricación crítica, que incluye todo lo que es la fabricación de vehículos, aviones, componentes ferroviarios, equipos electromecánicos, aceros. El resto estaba un poco repartido con porcentajes muy pequeños del sector nuclear, el transporte.

En 2014, los requerimientos de incidentes en energía bajaron a la mitad, al 32 %. En fabricación crítica subieron al 27 %, es decir, prácticamente igualando ambos ámbitos. Muy importante destacar que el 60 % (que también rondaban los trescientos) eran APT (amenazas persistentes avanzadas). ¿Por qué las empresas notifican incidentes? Pues por tres posibles razones: por concienciación, porque estás obligado a hacerlo o porque hayas tenido un problema tan grave que necesites que alguien te ayude a solventarlo y por eso necesitas transmitirlo.

Más interesantes aún son los datos de 2015. Ese año, se reparten un poco más. La energía baja otra vez a la mitad, al 16 %. La fabricación crítica aumenta al 33 %; es el más representativo. Por último, comenzamos a apreciar que otros sectores como el agua o el transporte cada vez dan más avisos. Si se hace un análisis de esta información, se muestra que hay más empresas de distintos sectores que lo están haciendo. Al principio, en 2013, prácticamente la mitad de las empresas que informaban eran del sector de la energía. Pero conforme ha ido pasando el tiempo, lo han ido haciendo más, y la legislación solo obliga al sector eléctrico a notificar. Por tanto, puede deberse a otro de los dos motivos que comentaba: a la concienciación o a que los problemas están siendo cada vez más graves.

Antonio Guzmán

A tu juicio, ¿cuál de los dos pesa más?

José Valiente

No te sabría decir en qué porcentajes. Seguramente los dos. Sí es cierto que la concienciación cada vez está siendo más importante a la hora de notificar, porque además es una de las claves para mejorar la ciberseguridad, la compartición de la información. Porque si esto no se hace así, lo vamos a tener muy difícil para resolver estos problemas.

En España también se ha hecho un gran esfuerzo desde el CERTSI, el CERT de Seguridad e Industria. Se han publicado algunos datos de eventos que han transmitido los incidentes en el ámbito de los sistemas de operaciones y sistemas industriales. Y el principal sector que informa de ellos es el de la energía, como ocurría en 2013 en Estados Unidos.

Elena García Díez

Los datos que mencionas de nuestro CERTSI, CERT de Seguridad e Industria, son resultado del análisis que hemos realizado sobre los avisos de seguridad publicados a lo largo de todo 2015, en el que hemos estrenado una sección de avisos específicos sobre sistemas de control industrial. Esta labor, que ya veníamos haciendo sin tanta profundidad desde hace años en INCIBE, en 2015 se ha realizado con una profesionalidad específica y un acercamiento integral a la problemática de los avisos de control industrial, que nos ha permitido este año hacer este diagnóstico. Ver realmente cuáles son no el tipo de incidentes, pero sí las alertas o las problemáticas que ha habido o han tenido presencia en el ámbito del control industrial. Las conclusiones y cifras en este ámbito son efectivamente las que ha resumido José.

José Valiente

Efectivamente, y hecha esa matización, lo cierto es que el sector de la energía sigue apareciendo como el que más avisos realiza por el tipo de tecnología. Luego le sigue el sector del agua y el de la alimentación. Este último, que puede sorprender, tiene todo el sentido del mundo. En el sector de la alimentación se utilizan muchos procesos químicos y utilizan tecnología que se emplea también en entornos petroquímicos, susceptibles de esta problemática.

Antonio Castillo

Yo creo que has dado el punto de vista complementario. Además, como ha habido una interacción muy fructífera a lo largo de toda la jornada, creo que estos datos nos centran dónde están apareciendo los problemas y también un poco en qué proporción.

Está claro, como tú decías, que hay un aspecto de concienciación. De alguna manera esa es una de las cuestiones fundamentales. Probablemente se produce una especie de sentimientos encontrados. Si yo transmito a la gente lo que está ocurriendo, hasta qué punto se va a asustar y se va a producir una situación de péndulo que va a dirigirlo hacia el otro lado. Pero claro, también hay que ser conscientes de lo que está pasando.

Por eso, ahora creo que vamos un poco a insistir en estos aspectos desde una perspectiva con vistas al futuro. Para eso, agradecería la contribución de Antonio, de ElevenPaths. Queremos saber cómo se está plasmando esto en unas tecnologías que están surgiendo nuevas. Como el *Internet of Things* está confeccionando un nuevo sector para el que se están generando una serie de plataformas en las que no sabemos exactamente si se están teniendo en cuenta debidamente los aspectos de seguridad.

Tampoco podemos olvidar que Internet nació como una infraestructura que soportara todo tipo de ataques. Estábamos, y Miguel lo sabe muy bien, en plena Guerra Fría cuando se comenzó a popularizar. Lo que se quería era que ante un caso de ataque con misiles, con bom-

ba atómica, no se supiera dónde estaba el centro de mando. Ese fue el principio, porque la idea era en aquel momento que si tienes una red de otro tipo, que establece conexiones permanentes, tú sepas dónde está el centro de mando. Solo había que saber cuál era el punto con más conexiones permanentes. Pero si quitas las conexiones permanentes y son virtuales, no hay centro de mando y no sabes dónde está. Por tanto, estamos luchando contra un fenómeno, que en su momento nace para otro tipo de seguridad: un fenómeno que surgió de la bahía de Cochinos para que no nos atacaran con misiles; para eso era.



ANTONIO GUZMÁN

Director de Innovación de ElevenPaths

Preguntas a partir de las cuales se inició su intervención:

- ¿Cómo está evolucionando la tecnología para responder a las amenazas?
- ¿Cómo la llegada del IoT modifica el mundo de la seguridad industrial?
- ¿Cómo va a evolucionar el ecosistema de empresas dedicadas a la ciberseguridad?

Siendo un poco breve, porque creo que ya hay muchas cosas dichas, el concepto de *Internet of Things* tiene muchas definiciones en diferentes ámbitos. Podemos encontrar distintas implementaciones de *Internet of Things*, que no dejan de estar en un entorno corporativo y no dejan de ser cámaras de videovigilancia. También hay muchas integraciones en un entorno industrial que se están vendiendo bajo la bandera de *Internet of Things*. Por eso a mí me gustaría que, prescindiendo de todas esas definiciones, que creo que son fáciles de hallar, plantear lo que yo creo que, analizándolas todas, reúne un nuevo entorno que es muy desafiante. Sobre todo en busca de soluciones de ciberseguridad.

A la hora de discutir sobre el *Internet of Things*, si queremos quedarnos con su esencia, tenemos que nombrar la interconectividad. Nos referimos al Internet de las cosas, es decir, a conectarlo todo a un medio, que nos va a garantizar esa interconectividad entre los diferentes elementos con los que vamos a jugar. Pero esto ya lo teníamos antes. Al final no hay demasiada diferencia, hablamos de una interconectividad que ya existía. Pues ¿dónde está la diferencia? Rascando un poco todas las definiciones, hay tres aspectos fundamentales que nos permiten hablar de *Internet of Things* como si fuese un paradigma nuevo. Uno de ellos es la escala. Seguro que lo hemos oído todos, nos referimos a 20 billones de dispositivos, billones en lo americano; lo que no deja de ser una cantidad enorme de dispositivos todos conectados entre sí. Se trata de muchísima cantidad de dispositivos que van a trabajar, si no todos a la vez, sí en porcentajes muy altos de forma colaborativa. Esto de por sí revienta la resiliencia que comentábamos. Al final, lo que vamos a

necesitar son sistemas que tengan un rendimiento muy afinado. La escala es en sí un problema, pero la buena noticia (voy a ir lanzando buenas noticias) es que, al contrario de lo que puede sugerir la lectura de las diferentes notas de prensa que se leen por todas partes, de momento la escala no es una realidad. Es un hecho, sucederá, tarde o temprano lo hará y todos los que estamos aquí tendremos mil dispositivos conectados de los que seremos responsables. Pero hoy, eso no es verdad. Actualmente la mayoría de las conexiones se siguen haciendo de acuerdo con un protocolo conectado a IPV4; algunas conexiones sí que van con IPV6, pero todavía existe el concepto del concentrador, existen las redes NESS, tenemos parcelada la comunicación y, hoy, no existe un problema de escala. Eso sí, como venimos diciendo, es necesario que las soluciones que estamos planteando para garantizar la seguridad, y la gestión de este tipo de entornos, incorporen por diseño la característica de escala y lo que afecta a un mantenimiento de un entorno seguro en el Internet de las cosas.

Otro aspecto que he ido extrayendo de la recopilación de definiciones antes de venir aquí a contaros mis impresiones es el de la heterogeneidad. En algunas conversaciones previas hemos afirmado que en un entorno industrial hay muchos fabricantes de dispositivos. Pero también es cierto que en un entorno industrial, cuando se hace una integración, parece que se elige una rama de fabricantes, aunque la oferta sobre el papel es que hay muchos tipos de fabricantes de dispositivos, lo que, desde una perspectiva industrial, complicaría el cómo se va a gestionar ese parque de dispositivos. En los entornos industriales, al final se opta por un tipo de solución. Es como si se achicara el problema. Cuando estamos hablando de *Internet of Things*, esa heterogeneidad va a ser global. Habrá integración, obviamente, que ahí es donde tenemos el vínculo directo con todo lo que se está haciendo en el mundo industrial; habrá integraciones que tendrán una familia entera de dispositivos, pero esto va a tener que convivir con otras integraciones para las que se habrán tomado otro tipo de soluciones. Así, la heterogeneidad, sumada a la escala, va a ser un problema grave.

El tercer rasgo es el de la deslocalización. Va a haber una distribución global de dispositivos. No es únicamente por conveniencia económica, porque cuesta mucho cablearlo. Vamos a tener comunicaciones inalámbricas localizadas con ubicaciones muy dispersas, como la información que van a proveer sobre los usuarios y sobre los sistemas. Estamos hablando de un sistema deslocalizado y de gran escala, con una altísima heterogeneidad.

Esta deslocalización tiene además dos componentes que hacen muy difícil añadirle una capa de ciberseguridad. Típicamente, en un entorno industrial podemos aplicar determinadas soluciones, al menos en una de las partes, que nos permiten aprovecharnos de la seguridad física. Sin embargo, hay muchos entornos que están dentro del *Internet of Things*, como es el caso de las *smart cities* u otro tipo de ámbitos abiertos, donde muchos de esos dispositivos tienen una amplísima exposición. Nos referimos a unos sensores dispersos por una ciudad que van a interactuar directamente con los usuarios. Con lo cual, esa deslocalización además tiene unas connotaciones de exposición muy, muy elevadas. Nos complica todavía

más el problema y hace que el *Internet of Things* sea en sí mismo un paradigma y una definición concreta.

Otra cuestión fundamental, que también permite diferenciarlos de otros paradigmas computacionales y que está de alguna manera vinculada con esta deslocalización, es que muchas de las configuraciones, acciones o información que reportan esos sensores se hacen mezclándolos con fuentes de datos externas. Al final, cuando tú construyes una funcionalidad del *Internet of Things*, no es puramente un entorno controlado, como podría ser una planta industrial, donde sabes más o menos cuáles van a ser los flujos de datos que quieres controlar. Aquí, lo que quieres es incorporar determinados flujos de información, fuentes de datos externas, más o menos fiables, en tu flujo normal de información. Por eso surge una derivada muy interesante, que enlaza con lo que empezábamos diciendo al principio de esta reunión, y es que en el *Internet of Things* va a aparecer un rol que hasta ahora no había aparecido: el individuo. Un individuo que no tiene por qué interactuar con el sistema, pero sí se puede ver beneficiado o afectado, como el resto de los *players* que van a interactuar con él. Esto nos va a permitir introducir una derivada de adaptación, adaptativo de cómo se construye el Internet de las cosas. Es importante este rol, porque va a ser el que nos va a justificar esta inclusión de las fuentes de datos externas.

Miguel Pérez Subías

O sea que cada persona es un sensor en sí mismo.

Antonio Guzmán

Sí, pero incontrolable, tú no has hecho un *upload* de ese sensor. No es algo que controles.

Pero ¿cómo plantearíamos un esquema de solución para el *Internet of Things*? Desde luego hay algo que tenemos que entender: en la esencia de la definición estamos hablando de interconectividad. Antes lo hemos mencionado, también va a haber una ejecución con máquinas, y esas máquinas van a estar interconectadas. De alguna manera la protección que podemos establecer frente a amenazas tiene que hacerse en esa conexión. Debemos garantizar que la comunicación que se lleve a cabo —y es una comunicación plural entre dispositivos (*machine to machine, user to machin, machin to user*)—, se haga lo más segura. Tal vez, el primer nivel que debamos alcanzar en términos de protección, hablando de ciberseguridad, sea garantizar que esas comunicaciones sean lo más seguras posibles, obviamente, sin perjudicar el rendimiento global del sistema.

Para conseguir ese esquema de protección, actualmente y siendo realistas, sabiendo que el problema de escala todavía no es real, la tendencia ahora mismo es adaptar soluciones más o menos tradicionales a este esquema concreto. ¿A qué nos lleva esto? A hablar de procesos de detección, protección y prevención y a intentar introducir sistemas de respuesta.

Hemos comentado antes los tiempos de respuesta. Aquí lo que estamos haciendo es un *soft* de seguridad industrial. Es verdad que los tiempos a los que tenemos que ajustarnos en estos entornos no son ventanas de tiempo real, en que como mucho se puedan permitir unos segundos de respuesta. Pero, sin embargo, en algunas de las implementaciones del *Internet of Things* hay en peligro vidas humanas; por ejemplo, en las aglomeraciones de personas en una zona concreta. Por tanto, los tiempos de respuesta tienen que ser ajustados.

Lo que hay que hacer es adaptar esas soluciones de respuesta, de protección y de prevención para ser compatibles con estas nuevas características. El problema es que esto es necesario pero no suficiente. ¿Por qué? Por estas características complejas que poseen. A partir de ahora lo que hay que hacer es evolucionar todas esas soluciones, hacerlas compatibles con la escala, heterogeneidad e interconectividad; pero además necesitamos ir un paso más allá. Necesitamos que la balanza, que está más inclinada en términos de detección, permita avanzar en términos de prevención. Porque el problema de escala es un problema en sí y hay muchas posibles interacciones con muchos usuarios simultáneamente. Por lo que cuanto antes puedas detectar la posible traducción de una amenaza a un ataque concreto, más efectivo será un sistema de protección.

En esta línea, y enlazando con la segunda pregunta que me realizabas, se plantean diferentes estrategias en el mundo de la ciberseguridad. Las amenazas cada vez son más complejas, la sofisticación es enorme y una constante. Al contrario de lo que puede pasar con otros sistemas de evaluación de riesgo que todos tenemos en la cabeza, en el caso de la ciberseguridad el ritmo que impone la aparición de nuevas amenazas no es algo del todo previsible. Antes jugamos con el término de «presunto maleante» cuando hablábamos de alguien que podría atentar contra nuestro sistema. Pero es que es un hecho. De repente alguien ha encontrado una determinada vulnerabilidad en un sistema y lo que va a hacer es montar un modelo de negocio (ya no es el *hacker* romántico) para sacar el máximo lucro de esa vulnerabilidad y va a perpetrar un ataque masivo. Esto incluye las APT, incluye el *malware*, incluye el *ransomware*, lo incluye todo. El nivel de sofisticación no nos permite pensar en un pirata sentado en el sofá de su casa. No, nos estamos refiriendo a bandas organizadas. Estamos hablando de cibercrimen. Es crimen organizado que utiliza el medio digital.

Esto nos complica mucho la vida. Porque, claro, yo tengo mis mecanismos de detección, de prevención y de respuesta. Pero si quiero irme hacia la parte de prevención, como mínimo tengo que rastrear los *modus operandi* que emplean los atacantes. Y para eso, lo único que se puede hacer, o al menos la tendencia que hay ahora mismo en tecnologías de protección y ciberseguridad, es consumir cuantas más fuentes de información y aprovechar otros paradigmas de computación como es el *big data*, construido sobre el *flash computing* y determinadas técnicas de *machine learning*, etc. Resumiendo, lo que hace falta es consumir muchas fuentes para localizar singularidades. Normalmente esas singularidades lo que nos van a permitir es inclinar la balanza más hacia el lado de la prevención que hacia el de la detección.

Esto no es blanco y negro, las mismas técnicas se podrán utilizar para mejorar los sistemas de detección y agilizar los mecanismos de respuesta. Al final lo que tenemos es un esquema muy complejo, que a día de hoy todavía es viable, pero si no somos espabilados y solucionamos nuestras aplicaciones, se van a quedar muertas.

Antonio Castillo

El debate ha sido muy interesante, pero nos queda un tema. Por un lado está la dependencia de las infraestructuras críticas de todos estos sistemas que estamos viendo y, luego, también queremos saber cuál es el riesgo para la evolución económica.



ÁNGEL LEÓN ALCALDE

Vocal asesor de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información

Preguntas a partir de las cuales se inició su intervención:

- ¿Qué riesgos no tradicionales pueden aparecer en sectores críticos (energía, transporte...) para un país?
- ¿En qué medida no atender la ciberseguridad adecuadamente tiene riesgo para la evolución económica de un país y su desarrollo industrial?

Sobre las infraestructuras críticas, voy a comentar el tema regulatorio. Seguramente a lo mejor enfrió algunas esperanzas que pueda haber en este tipo de cuestiones. Porque las infraestructuras críticas son un concepto interpretable, muy interpretable, y en eso estamos, en interpretarlo.

En el marco comunitario tenemos una directiva que establece dos tipos de infraestructuras críticas: energía y transportes. Al hacer la transposición nacional, por cuestiones políticas y de oportunidad, se amplió la lista hasta trece sectores porque la directiva lo permitía al ser una directiva de mínimos. Por eso han aumentado hasta trece sectores, entre ellos el de alimentación, que se ha mencionado antes, pero también están, entre otros, la Administración pública, el sanitario, etc. Esto es muy positivo porque nos hemos dotado de unas herramientas que nos permiten establecer una especial protección o dotarnos de una serie de mecanismos para ir más allá de lo que se decidió en la normativa comunitaria. Conseguimos mejorar la protección de las infraestructuras críticas. Pero ¿qué son las infraestructuras críticas? Queda dentro de las materias reservadas y se basan en un concepto jurídico indeterminado: en la cadena de razonamiento se utiliza el concepto de «servicios estratégicos», no se define en ningún sitio pero ahí se utiliza como término intermedio.

Sin embargo, no dejamos de tener un instrumento para llegar a un nivel máximo de protección. Es solo un instrumento. Porque luego hay que desarrollar unos planes de protección de operador, y aprobarlos y, llegado el momento, modificarlos. Pero ¿quién aprueba la modifica-

ción? La Delegación del Gobierno del territorio en el que se ubica la infraestructura crítica. El concepto de infraestructura crítica adoptado en España sigue una perspectiva tradicional. Son infraestructuras que para empezar están establecidas en territorio nacional (todo lo que esté fuera dependerá de la Cooperación Internacional) y, además, fíjate si tenemos conciencia de que tiene que ser un concepto ligado al terreno, que la revisión de los planes la tiene que hacer la Delegación del Gobierno.

Además, las infraestructuras críticas incluyen todo aquello que pueda poner en riesgo la prestación de servicios. Por tanto, incluye riesgos informáticos, toda la ciberseguridad. Todo esto está bien, hemos ampliado las posibilidades, pero seguimos en una tendencia manifiestamente mejorable para gente que estamos en el sector TIC.

Otra carencia que tiene la normativa de infraestructuras críticas y que nos lo ha comentado el personal del CNPIC es que les gustaría tener la obligación y la garantía de que cuando haya un incidente, se notifique. De momento no existe la obligación. Por ello tenemos un problema. Porque ¿qué pasa con aquellos que tienen un incidente y afrontan riesgo-beneficio desde una perspectiva de riesgo reputacional? Sobre todo que un riesgo que ya ha pasado no suele reportarse.

Afortunadamente hemos aprobado o cerrado un acuerdo en la Unión Europea sobre esto, la Directiva NIS, que cubre más sectores, muchos más sectores de los que nosotros establecemos, aunque no todos los que hemos fijado. En esta directiva se decreta la obligatoriedad de dar aviso de incidentes. Eso sí, todo es muy interpretable. ¿Por qué? Porque nos encontramos de nuevo con un marco para definir los instrumentos, no con los instrumentos. Porque es a escala nacional donde se decide cuáles son cada uno de los servicios dentro de esos sectores esenciales. Estos servicios son importantes en toda la Unión Europea, pero no tienen por qué ser los mismos en todos los países. Pero ¿qué servicios concretos en cada uno de estos sectores? Queda la decisión al ámbito nacional. ¿La obligación de comunicar incidentes? Son las autoridades nacionales las que deciden cuándo un incidente es lo suficientemente importante como para tener la obligación de notificarlo. Un asunto que vuelve a aparecer entonces es la posibilidad de imponer obligaciones a los prestadores de estos servicios que se consideran esenciales, esto es, la imposición de unas obligaciones de seguridad, que también se decide a escala nacional.

Tenemos un mecanismo para establecer los mecanismos. Por consiguiente, tendremos un *metamecanismo*. Esto será la directiva cuando la transpongamos, veintiún meses desde que la adoptemos formalmente, pues aún no la hemos adoptado. Es un primer paso, antes no teníamos nada y ahora tenemos algo: colaboración entre países para compartir buenas prácticas. Y aporta un gran punto sobre la Ley de Infraestructuras Críticas. Porque la filosofía de la ley era solo la continuidad del servicio, que era un problema porque muchas veces el objetivo de los ciberdelincuentes es que el servicio no se interrumpa para seguir sacando dinero.

No fue fácil, hubo discusiones en Bruselas hasta que se convenció a los representantes de que cuando hablábamos de «seguridad» no lo hacíamos de «continuidad». Y borrar la palabra «continuidad», sustituirla por «seguridad», para asegurarnos, y añadir «integridad», «autenticidad», costó, pero se consiguió.

La Directiva NIS y la normativa sobre infraestructuras críticas son normativas complementarias o pueden ser complementarias, porque ambas se pueden desarrollar. Una es un meta-mecanismo y la otra es un mecanismo para establecer obligaciones de seguridad. Pero hay varias posibilidades para su implementación: pueden ir las dos de la mano, y hacemos que su supervisión dependa de un organismo grande y todopoderoso, o bien hacemos dos normativas separadas y cuando surjan conflictos entre ámbitos de competencias, que «se peleen» entre ministerios... Todas esas posibilidades están encima de la mesa.

Digamos que se demuestra que en el plano legislativo se va aprendiendo, se va tomando conciencia. La legislación debería ser el último recurso. Es más, siempre se le reprocha llegar tarde. A lo mejor es bueno. Dentro de veinte años, lo habremos reformado todo otra vez y será mejor aún. A mí me gustaría tener lo mejor desde el principio, pero esto conlleva un proceso de aprendizaje.

El gran riesgo que yo le veo es que queda un gran espacio a la interpretación. No solamente es un riesgo en abstracto, es que estamos hablando de cosas de seguridad que suenan mucho a seguridad nacional, a pesar de que se haya dicho en el texto que no lo es. Por tanto, no es solo que sea interpretable, sino que va a ser interpretado. Será interpretado de acuerdo con los diferentes intereses de todos aquellos que tenemos utilidades en la materia. Los incentivos que teníamos para la convergencia en las directivas de teleco, en este caso, no juegan de modo puro y hay más ruido. Un ruido que será mucho más difícil de filtrar. Ya veremos cómo evoluciona. De momento tenemos muy buena relación con el Ministerio del Interior, por lo que intentaremos ir con la convergencia de estos ingredientes que aporta la Directiva NIS para reforzar aquellas carencias que han detectado. Al final, trabajamos para la misma empresa y para los mismos clientes, sobre todo, que son los ciudadanos.

En cuanto a la segunda pregunta, el riesgo de la ciberseguridad para el desarrollo industrial de un país; la ciberseguridad es un peaje que tenemos que pagar por la introducción de las tecnologías de la comunicación y de la información. Esto no es una cuestión nacional, esto es una cuestión del modelo económico de los países entre los que nos encontramos. El problema es que si no se adopta un modelo o unos protocolos adecuados, no se saquen todos los beneficios que se deberían obtener de la introducción de las tecnologías de la información en la industria. Por eso, yo no sé qué es peor, que no se saque ese provecho porque haya miedos y no los potenciemos a fondo o que nos peguemos un tortazo y haya un retroceso. No sé cuál sería la peor de las cosas. El riesgo es básicamente ese; es un peaje que hay que pagar, pero deberíamos pagarlo en la medida necesaria.

¿La componente nacional? Muy limitada, únicamente encaminada a este tipo de cosas que he mencionado. Hay que ver hasta qué punto los Gobiernos o los Estados podemos ser un obstáculo para que los sectores industriales sepan solucionar estos problemas o, al contrario, que ayudemos a solucionarlos. Somos un agente intermedio. Estamos ahí porque tenemos el monopolio legal, la legislación es nuestra. Pero para bien o para mal estamos en medio. Intentaremos estorbar lo menos posible. No va más allá de lo que es la implementación de la legislación. El papel de la Administración debe ser el de establecer un equilibrio entre los diferentes agentes del mercado a la hora de dirimir sus conflictos.

Antonio Castillo

Pero, y un poco la pregunta es para todos, ¿hasta qué punto la posición en la legislación, en la normalización de los diferentes países (porque eso son capacidades y temas nacionales), influye en su aportación al desarrollo industrial de cada país en ese tema? ¿Por qué os lo pregunto? En la época en que conocía los programas de la Comisión Europea, todo los temas que tuvieran que ver con seguridad, comunicaciones de defensa, etc., y que aparecieran en alguno de los programas de desarrollo de la Unión Europea, automáticamente eran vetados por Francia. No encontraréis ningún proyecto, subvencionado, patrocinado, o cualquier otra cosa, relacionado con eso. Y es así desde los años setenta.

De alguna manera en las telecomunicaciones ha sido más fácil en el sentido de que el negocio estaba implantado en los países europeos de la misma forma. Lo mismo era, salvo en pequeños detalles, el negocio de Telefónica en España que el negocio de Orange. Cambiaba muy poco, prácticamente la única diferencia era la participación accionarial del Estado. Pero en esto, que hay una industria detrás, a mí no me da la impresión de que los países estén siendo neutrales en los problemas.

Ángel León Alcalde

Eso es a lo que me refería sobre la idea de que tener una directiva es un primer paso. Porque por fin nos hemos dado cuenta de que no podemos ir por libre. Pero la directiva va a salir de una forma mucho más descafeinada de lo que se pretendía inicialmente.

Obviamente ha habido claros posicionamientos, muy fuertes entre países en algunas posturas totalmente cerradas y contrarias a la introducción de estos procedimientos, y otros que teníamos una visión más europea. Pero también dependía mucho de quién fuera el representante del país. Porque las posiciones nacionales se construyen como se construyen. No nos engañemos. Por parte de España íbamos los del Ministerio de Industria, pero por parte de otros países iba gente relacionada con la seguridad nacional. Por eso, había determinadas posiciones dependiendo mucho de las personas. Otra cosa que influía era la situación de los intereses geoeconómicos y geopolíticos de los países. Todos los países de la órbita de Estados Unidos tenían más reticencias a la hora de incluir en la directiva cuestiones como Inter-

net. Si eran temas relacionados con agua, transportes y tal, estaba bien, pero todo lo que tenía que ver con Internet y las redes de la información nos costó mucho. Y entonces llegamos al punto de tener que preguntar: ¿cómo le explicamos a la ciudadanía que hemos hecho una Directiva Europea para proteger la seguridad de las redes y la información y que aquel elemento que es más visible para ellos no lo integramos? ¿Cómo se lo explicamos? ¿Por qué lo querían hacer? Pues por una serie de cuestiones industriales, culturales o geopolíticas; no lo sabemos muy bien. Por eso el hecho de que haya habido una primera directiva es un gran paso. Nosotros a escala nacional veremos cómo le sacamos el máximo provecho. Pero internacionalmente, y a pesar de que va a tener unos efectos mucho menores de los que nos habíamos esperado (incluida la propia Comisión Europea), va a aportar bastante, y no va a ser papel mojado. Hemos superado un poco esa barrera de que todo aquello que tuviera que ver con seguridad era materia nacional.

Manuel Escalante García

Hay un fiel reflejo de esto, y estoy muy de acuerdo contigo en lo de que no estamos dispuestos a ceder en este tipo de materias en la Agencia Europea de Seguridad de las Redes y la Información (ENISA). Nació como el organismo europeo de seguridad, yo estuve en el Consejo de Administración algunos años, y allí era imposible llegar a algún acuerdo. ENISA se ha convertido en un magnífico Departamento de Estudios. Porque cuando se proponía cualquier iniciativa que tuviera visos de poder socavar la soberanía nacional de cualquier país, había pie con pared por aquellos que no necesitaban a nadie para protegerse. Es un fiel reflejo de esta situación: como tiene que ver tanto con temas de seguridad nacional, se ha quedado totalmente descafeinado. Nos pasábamos los Consejos de Administración discutiendo sobre temas de recursos humanos. Era desesperante porque allí estábamos para otro asunto.

Una pregunta que tenía que realizarte sobre la Directiva NIS. En la Directiva NIS hay un aspecto que a mí me parece particularmente interesante sobre las autoridades nacionales competentes. Aunque me gustaría saber quién va a ser mi interlocutor. Es un problema al que yo me he enfrentado en muchísimas ocasiones. ¿Con quién tengo que hablar? Por eso me gustaría saber cómo lo están resolviendo a escala europea y hacia qué lado se está decantando el tema.

Ángel León Alcalde

Todavía no hemos adoptado la directiva. Según lo que vaya a ser, se va a tener que designar la autoridad nacional competente. Aquí lo importante será el primer término: esa autoridad, quién ejerce la autoridad sobre ti, quién te va a poder obligar a tomar determinadas medidas de seguridad y a quién se van a tener que transmitir los incidentes. En el ámbito nacional, cada quién decidirá cómo hacerlo.

Un caso de aproximación, si quisierais, es la Directiva de Infraestructuras Críticas. En esa directiva también se establece una autoridad competente. ¿Puede ser la misma autoridad competente? Yo veo varias posibilidades y todas ellas con diferentes problemáticas. Porque ¿puede una misma autoridad saber qué medidas adoptar en un hospital, un banco o en una eléctrica? Desde este punto de vista a lo mejor resulta más conveniente otorgar más competencias a autoridades sectoriales como sería la CNMC, el Ministerio de Sanidad, el Banco de España... Sería otra posibilidad, pero surge el problema de cómo garantizo la coherencia en ciberseguridad entre todos ellos. O, por ejemplo, creo una Agencia de Protección de Seguridad. Pero, claro, entonces cuando surge un problema de ciberseguridad, a lo mejor el operador tiene que comunicarlo a la Agencia de Protección de Datos, a la nueva agencia de ciberseguridad y al «Ministerio de no sé qué» porque es la red de telecomunicaciones; es la misma información para tres sitios. Sería más lógico que todo fuera al mismo. Esta es mi preocupación a corto plazo, porque veo tres modelos y un problema de gobernanza.

Desde mi punto de vista, es una directiva de mínimos, por lo que se va a ir más allá. Por tanto, primero habrá que ver cuánto más allá vamos a ir. Ver cuál es la gestión que hay que hacer y a partir de eso determinar el modelo de gobernanza. Porque, al final, la Administración es rozamiento, como la mecánica. El rozamiento es una bendición porque sin él no pararíamos nunca. Somos «un mal», pero un mal necesario. No sé cuál será la solución más adecuada. Puede ser que pondría en tercer lugar el modelo de agencia.

Paloma Llanea

A mí me gustaría hacer una petición. Lo que le preocupa a mi clientela es la existencia de varios regímenes sancionadores sobre los mismos hechos. Es decir que esta es otra de las cuestiones fundamentales: he tenido un problema, lo he tenido que notificar a esta organización para que me sancionen y a esta otra también para que me vuelvan a sancionar. Yo pediría que se cumpliera el *non bis in ídem* alguna vez. Que se pongan de acuerdo y sancionen solo una vez. Porque la gente no hace más que preguntarme cuánto me va a costar esto y cuánto voy a tener que provisionar.

Ángel León Alcalde

Por eso digo que la acción de una nueva agencia me parece la menos preferible. Pero la verdad es que no lo descarto.

